UNIVERSIDADE FEDERAL DO PARANÁ

DANIEL TEMPSKI FERREIRA DA COSTA

A PRODUÇÃO E ADMISSIBILIDADE DA PROVA PENAL DIGITAL DOTADA DE CRIPTOGRAFIA PONTA A PONTA: A EXPERIÊNCIA DO DIREITO COMPARADO E SEUS REFLEXOS NO ORDENAMENTO JURÍDICO BRASILEIRO

CURITIBA

2023

DANIEL TEMPSKI FERREIRA DA COSTA

A PRODUÇÃO E ADMISSIBILIDADE DA PROVA PENAL DIGITAL DOTADA DE CRIPTOGRAFIA PONTA A PONTA: A EXPERIÊNCIA DO DIREITO COMPARADO E SEUS REFLEXOS NO ORDENAMENTO JURÍDICO BRASILEIRO

Dissertação apresentada como requisito parcial à obtenção do título de Mestre em Direito do Estado, Setor de Ciências Jurídicas, da Universidade Federal do Paraná.

Orientador: Prof. Dr. João Gualberto Garcez Ramos

CURITIBA
2023

DADOS INTERNACIONAIS DE CATALOGAÇÃO NA PUBLICAÇÃO (CIP)
UNIVERSIDADE FEDERAL DO PARANÁ
SISTEMA DE BIBLIOTECAS – BIBLIOTECA DE CIÊNCIAS JURÍDICAS

Costa, Daniel Tempski Ferreira da
A produção e admissibilidade da prova penal digital dotada de criptografia ponta a ponta: a experiência do direito comparado e seus reflexos no ordenamento jurídico brasileiro / Daniel Tempski Ferreira da Costa. – Curitiba, 2023.
1 recurso on-line : PDF.

Dissertação (Mestrado) – Universidade Federal do Paraná, Setor de Ciências Jurídicas, Programa de Pós-graduação em Direito.
Orientador: João Gualberto Garcez Ramos.

1. Prova criminal. 2. Prova digital. 3. Criptografia. 4. Direito comparado I. Ramos, João Gualberto Garcez. II. Título. III. Universidade Federal do Paraná.

Bibliotecária: Eglem Maria Veronese Fujimoto – CRB-9/1217

TERMO DE APROVAÇÃO

Os membros da Banca Examinadora designada pelo Colegiado do Programa de Pós-Graduação DIREITO da Universidade Federal do Paraná foram convocados para realizar a arguição da Dissertação de Mestrado de **DANIEL TEMPSKI FERREIRA DA COSTA** intitulada: **A produção e admissibilidade da prova penal digital dotada de criptografia ponta a ponta: a experiência do Direito Comparado e seus reflexos no ordenamento jurídico brasileiro**, sob orientação do Prof. Dr. JOÃO GUALBERTO GARCEZ RAMOS, que após terem inquirido o aluno e realizada a avaliação do trabalho, são de parecer pela sua APROVAÇÃO no rito de defesa.

A outorga do título de mestre está sujeita à homologação pelo colegiado, ao atendimento de todas as indicações e correções solicitadas pela banca e ao pleno atendimento das demandas regimentais do Programa de Pós-Graduação.

CURITIBA, 29 de Março de 2023.

Assinatura Eletrônica
29/03/2023 16:23:01.0
JOÃO GUALBERTO GARCEZ RAMOS
Presidente da Banca Examinadora

Assinatura Eletrônica
29/03/2023 17:03:57.0
GUILHERME BRENNER LUCCHESI
Avaliador Interno (UNIVERSIDADE FEDERAL DO PARANÁ)

Assinatura Eletrônica
30/03/2023 14:56:07.0
MARION BACH
Avaliador Externo (FAE - CENTRO UNIVERSITÁRIO)

ATA Nº299

ATA DE SESSÃO PÚBLICA DE DEFESA DE MESTRADO PARA A OBTENÇÃO DO GRAU DE MESTRE EM DIREITO

No dia vinte e nove de março de dois mil e vinte e tres às 10:00 horas, na sala 317 - Ruy Corrêa Lopes - Sala de Defesas - 3º Andar, Prédio Histórico da UFPR - Praça Santos Andrade, 50, foram instaladas as atividades pertinentes ao rito de defesa de dissertação do mestrando **DANIEL TEMPSKI FERREIRA DA COSTA**, intitulada**: A produção e admissibilidade da prova penal digital dotada de criptografia ponta a ponta: a experiência do Direito Comparado e seus reflexos no ordenamento jurídico brasileiro**, sob orientação do Prof. Dr. JOÃO GUALBERTO GARCEZ RAMOS. A Banca Examinadora, designada pelo Colegiado do Programa de Pós-Graduação DIREITO da Universidade Federal do Paraná, foi constituída pelos seguintes Membros: JOÃO GUALBERTO GARCEZ RAMOS (UNIVERSIDADE FEDERAL DO PARANÁ), GUILHERME BRENNER LUCCHESI (UNIVERSIDADE FEDERAL DO PARANÁ), MARION BACH (FAE - CENTRO UNIVERSITÁRIO). A presidência iniciou os ritos definidos pelo Colegiado do Programa e, após exarados os pareceres dos membros do comitê examinador e da respectiva contra argumentação, ocorreu a leitura do parecer final da banca examinadora, que decidiu pela APROVAÇÃO. Este resultado deverá ser homologado pelo Colegiado do programa, mediante o atendimento de todas as indicações e correções solicitadas pela banca dentro dos prazos regimentais definidos pelo programa. A outorga de título de mestre está condicionada ao atendimento de todos os requisitos e prazos determinados no regimento do Programa de Pós-Graduação. Nada mais havendo a tratar a presidência deu por encerrada a sessão, da qual eu, JOÃO GUALBERTO GARCEZ RAMOS, lavrei a presente ata, que vai assinada por mim e pelos demais membros da Comissão Examinadora.

Observações: A banca examinadora decidiu pela aprovação do candidato e recomendação de publicação do trabalho.

CURITIBA, 29 de Março de 2023.

Assinatura Eletrônica
29/03/2023 16:23:01.0
JOÃO GUALBERTO GARCEZ RAMOS
Presidente da Banca Examinadora

Assinatura Eletrônica
29/03/2023 17:03:57.0
GUILHERME BRENNER LUCCHESI
Avaliador Interno (UNIVERSIDADE FEDERAL DO PARANÁ)

Assinatura Eletrônica
30/03/2023 14:56:07.0
MARION BACH
Avaliador Externo (FAE - CENTRO UNIVERSITÁRIO)

RESUMO

Esta dissertação trata da produção e admissibilidade da prova penal digital protegida pela criptografia ponta a ponta (E2EE). O objetivo geral é sistematizar as divergentes informações sobre um dos maiores problemas da atualidade advindos da implementação da E2EE: compatibilizar a privacidade das comunicações digitais e manter importante poder do Estado de resguardo da segurança pública. Em vista disso, primeiramente, chegou-se à conclusão de que existem falhas no sistema da E2EE, possibilitando, através de estratégias investigativas alternativas, a realização de sua interceptação telemática. Ao mesmo tempo, verificou-se que determinar a proibição da E2EE às empresas privadas (*Big Techs*) é uma utopia, pois geraria a busca por aplicativos semelhantes que prezam a clandestinidade, ou outros meios para criptografar mensagens. Ademais, já há previsão técnica de tecnologias futuras em que serão possíveis realizar a quebra da criptografia ponta a ponta atual, como a computação quântica. Importantes Nações já perceberam que uma maneira eficaz em conciliar os interesses de ambas as partes é a busca da cooperação das empresas privadas detentoras dessa tecnologia com o Estado, desencadeando-se o modelo de "proceduralização" do direito, para que aquelas forneçam a estrutura necessária para algum controle das provas penais digitais, não escapando a imposição de normas de responsabilidades às pessoas jurídicas. Nessa linha, observou-se que é indissociável ao sucesso do combate à criminalidade a cooperação jurídica internacional e um sistema jurídico globalizado, pois as novas tecnologias não obedecem às fronteiras, com destaque à Convenção de Budapeste. Outro objetivo deste trabalho, portanto, através do método do direito comparado, foi o de procurar as eventuais soluções dessa crise na doutrina, legislação e jurisprudência de outros países, porque o problema é universalizado (coerência fática e normativa). Iniciou-se pelos EUA, no qual há julgamentos por sua Suprema Corte sobre a mutação constitucional da sua 4ª emenda e o uso da inovadora Teoria do Mosaico, e, como isso repercutiu na legislação do país. Na mesma seara, investigou-se proposta de lei em tramitação do Reino Unido. Na Alemanha, tratou-se da interceptação telemática da prova digital criptografada devido à alteração do CPP alemão para possibilitar o uso de cavalos de Troia do Estado, mantida a E2EE e independentemente de qualquer cooperação privada. Quanto ao Brasil, buscou-se tecer exame crítico de julgamento iniciado na Suprema Corte em ações constitucionais (ADPF 403 e ADI 5527) que tratam da E2EE, além de outros julgados do STJ. Por fim, foram avaliados diversos projetos de lei brasileiros sobre o objeto da pesquisa, para uma análise comparativa à experiência estrangeira e nacional, objetivando a alteração da legislação processual penal brasileira de uma forma geral e prévia, evitando-se a persecução criminal ilícita.

Palavras-chave: prova penal digital; criptografia ponta a ponta; direito comparado; responsabilidades das *big techs*; legalização.

ABSTRACT

This dissertation deals with the production and admissibility of digital criminal evidence protected by end-to-end encryption (E2EE). The general objective is to systematize the divergent information about one of the biggest problems of today arising from the implementation of the E2EE: to make compatible the privacy of digital communications and maintain the State's important power of safeguarding public security. First, it was concluded that there are flaws in the E2EE system, making it possible, through alternative investigative strategies, to carry out telemetric interception. At the same time, it was found that it is utopian to ban the E2EE for private companies (Big Techs), since this would lead to a search for similar clandestine applications, or other means of encrypting messages. Moreover, there are already technical predictions of future technologies that will be able to break the current end-to-end encryption, such as quantum computing. Important nations have already realized that an effective way to reconcile the interests of both parties is to seek the cooperation of private companies that own this technology with the State, setting in motion the model of "proceduralization" of law, so that they can provide the necessary structure for some control over digital criminal evidence, not avoiding the imposition of liability rules on legal entities. Along these lines, it was observed that international legal cooperation and a globalized legal system are inseparable to the success of the fight against crime, since new technologies do not obey borders, with emphasis on the Budapest Convention. Another objective of this work, therefore, through the comparative law method, was to seek possible solutions to this crisis in the doctrine, legislation and jurisprudence of other countries, because the problem is universalized (factual and normative coherence). It started with the United States, where the Supreme Court has ruled on the constitutional mutation of its 4th amendment and the use of the innovative Mosaic Theory, and how this had repercussions on the country's legislation. In the same field, it dealt with a bill in progress in the United Kingdom. In Germany, we dealt with the telematic interception of encrypted digital evidence due to the alteration of the German CPP to allow the use of state Trojan horses, maintaining the E2EE and regardless of any private cooperation. As for Brazil, a critical examination was made of the judgment initiated by the Supreme Court in constitutional actions (ADPF 403 and ADI 5527) that deal with the E2EE, as well as other judgments of the STJ. Finally, several Brazilian bills on the subject of the research were evaluated for a comparative analysis of the foreign and domestic experience, with the aim of changing the Brazilian criminal procedure legislation in general and in advance, in order to avoid unlawful criminal prosecution.

Keywords: digital criminal evidence; end-to-end encryption; comparative law; responsibilities of big techs; legalization.

LISTA DE SIGLAS

ADI	Ação Direta de Inconstitucionalidade
ADPF	Arguição de Descumprimento de Preceito Fundamental
ALPRS	Automated license plate readers
ANATEL	Agência Nacional de Telecomunicações
CADH	Convenção Americana de Direitos Humanos
CEDH	Convenção Europeia de Direitos Humanos
CF	Constituição Federal
CIDH	Corte Interamericana de Direitos Humanos
CP	Código Penal brasileiro
CPP	Código de Processo Penal brasileiro
CSLI	Cell site location information
E2EE	End-to-end encryption
EARN IT Act	Eliminating Abusive and Rampant Neglect of Interactive Technologies Act
ECPA	Electronic Communications Privacy Act
FBI	Federal Bureau of Investigation
INSS	Instituto Nacional do Seguro Social
LGPD	Lei Geral de Proteção de Dados Pessoais
LGPDP	Lei Geral de Proteção de Dados Pessoais - Penal
MCI	Marco Civil da Internet
MPSP	Ministério Público do Estado de São Paulo
NSA	National Security Agency
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
TEDH	Tribunal Europeu de Direitos Humanos
TJ	Tribunal de Justiça
TJSP	Tribunal de Justiça de São Paulo
TNU	Turma Nacional de Uniformização
TR	Turma Recursal
TRF	Tribunal Regional Federal
TSE	Tribunal Superior Eleitoral

SUMÁRIO

1 INTRODUÇÃO

Em uma visão inicial ampla, pois o tema é complexo e circula por distintos caminhos naturais da sociedade, não só em seu âmbito interno, mas integrado ao mundo globalizado, é fato que o estudo da prova penal está em robusta transformação, assim como as incertezas advindas ao redor de mudanças sociais ocasionadas pelas novas tecnologias utilizadas de forma diária para as mais diversas e usuais atividades em conexão por bilhões de pessoas. Dessa maneira, acabam os dados dessas novas tecnologias, especialmente os relativos à comunicação, servindo como fonte de prova[1] para eventual resolução de conflitos, mas, de uma forma nunca vista, originária de uma nova era de conexão digital de acelerada difusão das formas de mensageria privada.

Diante deste panorama, esta dissertação irá tratar, preponderantemente, de imbróglio polêmico e de magnitude internacional: as provas digitais dotadas de criptografia ponta a ponta (E2EE) e seu uso para a persecução penal de aplicativos de mensagens desenvolvidos pelas chamadas *Big Techs*, tais como: o WhatsApp (pertencente ao Facebook, ou, Meta), o iMessage (da Apple) e o Skype (da Microsoft), todas empresas com sede nos Estados Unidos da América (EUA).

Tratar da criptografia ponta a ponta foi, desde o início, o mote principal desta pesquisa científica, mas que logo demandou estudo ramificado por outras searas, notadamente sobre termos científicos ligados à informática e modernas técnicas de investigação penal digital, sem contar os incursos necessários pela legislação, doutrina e jurisprudências de diversas **N**ações. Sem isso, não há como se ter uma noção de todo o problema e eventuais possibilidades, soluções e críticas, mantido o cuidado de não desviar do incurso original do trabalho; porém, foram pontos obrigatórios de pesquisa para uma visão completa às perguntas investigativas e eventuais respostas divergentes surgidas no desenvolvimento.

Várias questões em torno do objeto principal de pesquisa são expostas na jurisprudência e legislação, posta e proposta, de outros países, como os EUA, Reino

---

[1] GOMES FILHO, Antônio Magalhães. Notas sobre a terminologia da prova (reflexos no processo penal brasileiro). In: YARSHELL, Flávio Luiz; MORAES, Maurício Zanoide de (Org.). **Estudos em homenagem à Professora Ada Pellegrini Grinover**. São Paulo: DPJ, 2005, p. 303-318. Em referência à diferenciação entre os conceitos de fonte de prova, meios de prova (endoprocessual) e meios de investigação (ou de pesquisa) de prova (em geral, extraprocessuais), com distintas repercussões em casos de irregularidade nestas duas últimas.

Unido e Alemanha, especialmente selecionados por questões sociopolíticas, econômicas e estratégias diferenciadas em relação à prática investigativa criminal para acesso a tais mensagens criptografadas. Mas não se limita a isso o trabalho. Deve-se ter em mente que além de polêmicas jurídicas dentro de cada país e de sua relação com inúmeros outros para a colaboração probatória internacional, dado o processo de globalização na comunicação digital, há questões de ordem prática que merecem um mínimo exame panorâmico, justamente visando à efetividade de uma ou outra solução ao problema principal proposto, em síntese: resolver, ou, no mínimo, uniformizar de alguma maneira possível, o conflito de interesses de relevantes direitos e garantias fundamentais, como, de um lado, o direito à privacidade, intimidade, livre manifestação do pensamento e o sigilo das comunicações telefônicas e telemáticas, e, de outro, a segurança pública, inseridos em uma nova concepção de sociedade global-digital.

Ilustre-se desde agora uma dessas complexidades práticas, almejando uma visão mais abrangente da polêmica principal, um aclaramento ao leitor. Diz respeito à existência de organizações estabelecidas como desenvolvedoras de tecnologia de mensagens via aplicativos móveis dotados da E2EE, voltadas à venda a criminosos por maneiras alternativas àquelas dos usuários em geral de aplicativos de mensagens criptografadas, como o WhatsApp. Contra tais empreendimentos já há estratégicas repressões dos governos. Numa delas, o FBI, na operação *Trojan Shield*, prendeu diversos criminosos por todo o mundo, ao criar um negócio de fachada prometendo a venda de telefones criptografados, mas aos quais tinha total acesso[2]. Ora, com esse breve caso, quer-se demonstrar que não se pode limitar a pesquisa à atuação e responsabilidades das *Big Techs*, pois o problema é mais alargado; e a questão de defesa da segurança nacional ("circunstâncias exigentes"), destarte, é mais uma dos diversos pontos que serão objeto de investigação científica, dados os subterfúgios de se elencarem exceções a garantias constitucionais ligadas ao sigilo de comunicações telefônicas e telemáticas recorrentes pela própria Suprema Corte de países democráticos.

---

[2] THE UNITED STATES ATTORNEY'S OFFICE. Department of Justice. U.S. Attorney's Office. FBI's Encrypted Phone Platform Infiltrated Hundreds of Criminal Syndicates; Result is Massive Worldwide Takedown. **Federal Bureau of Investigation**, 8 jun. 2021. Disponível em: https://www.justice.gov/usao-sdca/pr/fbi-s-encrypted-phone-platform-infiltrated-hundreds-criminal-syndicates-result-massive. Acesso em: 26 nov. 2021.

Há, ainda, como fato ilustrativo tangente, mas embutido como necessário à demonstração por onde andará a pesquisa, a situação do popular aplicativo de mensageria privada denominado Telegram[3], o qual, declaradamente, não cumpre decisões judiciais para a investigação de delitos, limitando-se sua cooperação a seu livre arbítrio; e daí a justificada preocupação das autoridades a este momento singular da comunicação digital, que promete alterar boa parte da forma com que antes pensávamos diversas regras do direito. A política da empresa é clara no sentido de desobedecer a decisões judiciais em prol da privacidade, com apenas uma ressalva, até hoje não usada.[4]

Exposto esse cenário das preocupações que giraram em torno desta pesquisa, verifica-se que os EUA deve ser o foco principal, não por mera coincidência, ou por ser a maior potência mundial por amplos aspectos, mas pelo impacto que suas decisões, advindas dos Poderes Executivo, Legislativo e Judiciário, terão em todo o mundo. Como dito, é o país sede das *Big Techs*, ou seja, decisões judiciais e novas legislações terão reflexos imediatos, ao menos de execução facilitada; há o uso frequente de seus precedentes judiciais no Supremo Tribunal Federal brasileiro (STF)[5], e, consequentemente, suas inovações teórico-jurídicas atreladas à persecução criminal frente às novas tecnologias repercutirão no Brasil e no resto do mundo, até por uma coerência na matéria fática de origem; por fim, há legislações postas e propostas diretamente ligadas à E2EE em ampla discussão por esse país. Tudo isso merece, portanto, ser explorado nesta dissertação.

O novo panorama principal estabelecido no ordenamento jurídico norte-americano é a mutação constitucional da 4ª emenda da sua Constituição, em razão de mudanças sociais advindas da tecnologia na investigação criminal e, outrossim, a

---

[3] O Telegram mudou-se da Rússia para Dubai, pois bloqueado (2018) após a regulamentação russa da criptografia em 2016 e sua recusa em quebrá-la. Cf.: MUNCASTER, Phil. Telegram App Banned in Russia. **Infosecurity**, 16 abr. 2018; FUNDAÇÃO GETÚLIO VARGAS (FGV). **CryptoMap**: uma pesquisa sobre o debate jurídico da criptografia. Disponível em: https://www.fgv.br/direitosp/cryptomap/#home. Acesso em: 29 nov. 2021.

[4] Diz a empresa que "só pode ser forçada a entregar dados se um assunto for grave e universal o suficiente para passar pelo escrutínio de vários sistemas jurídicos diferentes em todo o mundo. Até hoje, nós divulgamos 0 bytes de dados de usuários para terceiros, incluindo governos". Cf.: TELEGRAM. **Perguntas frequentes**. Disponível em: https://telegram.org/faq?setln=pt-br. Acesso em: 18 nov. 2022.

[5] Sobre a influência do direito norte-americano e alemão nos Acórdãos do STF, chamando atenção o autor a um maior dever de cuidado no uso do direito comparado por conta de exemplos malsucedidos. Vide: BORGES, Ademar. O direito estrangeiro no aperfeiçoamento da jurisdição constitucional brasileira. **Jota**, 16 nov. 2021. Disponível em: bit.ly/3Yfn6F4. Acesso em: 19 nov. 2021.

busca por um consenso da colocação cooperativa do setor privado (empresas de tecnologia) para a construção de meios aptos à produção da prova digital ao Estado dentro de sua função constitucional de persecução penal. Mas há ainda outros apontamentos advindos do estudo de leis, em vigor ou em construção legislativa, do Reino Unido e Alemanha, tudo isso com o escopo de aplicação ao Brasil através do método de investigação classificado como direito comparado "funcionalista"[6], voltado à sistematização universal em matéria de cooperação jurídica internacional. E aqui cabe a advertência do cuidado tomado nesta dissertação, no uso do direito comparado, de que não há que se falar em simples "transplantes jurídicos", significando que as ideias expressas nas palavras conseguem migrar, mas não são transplantadas, "não se deslocam e criam raízes em seu novo ambiente sem ser modificadas de alguma forma"[7], pelo contrário.

Assim, há perspectivas investigativas de diferentes países, não só do ponto de vista do direito processual penal, mas também do direito penal. A quantidade e o emaranhado de divergências de informações técnicas dos especialistas em informática e das principais empresas de tecnologia, tal como a visão jurídica e ideológica, ora pela defesa, ora pela rejeição da segurança irrestrita na troca de dados criptografados entre os usuários, merecem organização para posteriores conclusões imparciais.

O problema é colossal e já anunciado como o maior a ser resolvido na atualidade entre poderosas Nações e as *Big Techs*. Nesse sentido e voltado à interação entre as ciências criminais e as novas tecnologias, o renomado Professor Dr. Ricardo Campos, da Universidade de Frankfurt, destaca mudanças importantes na Alemanha, na toada de projetos de lei semelhantes por vários países da Europa, EUA e Brasil, porquanto decorrente de um mesmo fenômeno mundial, não uma mera importação de normas[8].

---

[6] Pois "pretende identificar respostas jurídicas similares ou distintas, em conflitos sociais que se assemelham mesmo ocorrendo em lugares distintos no mundo", mas cuja solução legal dos problemas "possui uma 'equivalência funcional', já que "praticamente idênticos". In: DUTRA, Deo Campos. Método(s) em direito comparado. **Revista da Faculdade de Direito – UFPR**, Curitiba, v. 61, n. 3, set./dez. 2016, p. 198. Disponível em: bit.ly/3VXLgmg. Acesso em: 10 ago. 2021.

[7] Cf.: LEGRAND, Pierre. A Impossibilidade de "Transplantes Jurídicos". Tradução: Gustavo Castagna Machado. **Cadernos do Programa de Pós-Graduação em Direito/UFRGS**, Porto Alegre, v. 9, n. 1, 2014, p. 11. Disponível em: bit.ly/3hk05jL. Acesso em: 08 dez. 2021.

[8] "O debate brasileiro (assim como o alemão e de diversos outros países) é reflexo de um movimento global de adaptação do Direito às novas condições postas pela economia digital". Cf.: CAMPOS, Ricardo. Lei alemã ou movimento global? O debate sobre regulação de redes contextualizado. **Consultor Jurídico**, 24 nov. 2020. Disponível em: bit.ly/3BsSRRA. Acesso em: 20 nov. 2021.

Para tentar sistematizar toda essa teia de dados e celeumas, o presente estudo irá partir, no capítulo 2, da análise da crise global às investigações criminais gerada pela criptografia ponta a ponta nas plataformas digitais e aplicativos de mensagens, com incursos pelo seu conceito, aspectos técnicos da informática, sua relevância às garantias e direitos constitucionais em amplos e divergentes aspectos. Em seguida, tendo o WhatsApp como objeto de estudo, serão expostas as pesquisas apontando se existem e, caso positivo, quais são as falhas de sua segurança à leitura por terceiros não interlocutores, a fim de se ponderar os elementos influenciadores ao julgamento a favor e contra as teses opostas entre as *Big Techs* e diversas Nações e, ao final, encontrar dados mais claros e organizados se deve preponderar a manutenção ou a quebra da criptografia ponta a ponta, incluindo a contribuição da Teoria da Ação Significativa, desenvolvida pelo saudoso jurista e Professor catedrático da Universidade de Valência, Dr. Tomás Salvador Vives Antón, com objetivo de buscar soluções ao Brasil do inarredável problema da responsabilidade penal das pessoas jurídicas.

Como necessário e decisivo componente a uma conclusão mais acertada, a procura de lições jurisprudenciais, legislativas e doutrinárias no direito comparado é imprescindível, buscando-se, no capítulo 3, ensinamentos dos EUA, Reino Unido e Alemanha, sem prejuízo de pontuais referências de outros países.

Assim, com fulcro no direito comparado se buscará traçar, no terceiro capítulo, o tratamento da interceptação telemática das provas penais digitais dotadas da E2EE, sem esquecer-se da mutação constitucional da 4ª emenda dos EUA, da qual deriva toda uma inovadora ordem de atuação jurisdicional e legislativa sob a égide da denominada Teoria do Mosaico, utilizada como mote à análise de ofensa, ou não, a garantias constitucionais na investigação criminal. No estudo do tema no Reino Unido, haverá a apreciação de projeto de lei que promete burlar a E2EE por tecnologia alegadamente inovadora. Quanto ao incurso no ordenamento jurídico da Alemanha, além da legislação já vigente sobre a interceptação telemática por meios alternativos de investigação probatório-criminal digital, independentes de cooperação das empresas responsáveis pelos serviços de mensageria privada, será tratado novo conceito doutrinário a ver com tal interação em uma nova sociedade baseada nas plataformas digitais, chamado de modelo de "proceduralização" do direito.

Encerrando o incurso basal acerca do direito comparado, no capítulo 4 será tecido diagnóstico mediante a abordagem da doutrina e jurisprudência existentes no

Brasil e os novos projetos de lei aqui em desenvolvimento, os quais serão estudados com supedâneo crítico à experiência internacional, quando pertinente, exatamente pela integração comunicativa mundial, com extensão à repercussão da Convenção de Budapeste[9] ao tratar da cooperação jurídica em matéria probatória penal.

Calha mencionar que, apesar de estar em andamento no STF ações constitucionais que tratam exatamente da E2EE em aplicativo de mensageira privada (ADPF 403 e ADI 5527), a pesquisa não tem como objetivo exarar um mero parecer de tal e qual sentido nossa Suprema Corte deve seguir (tendo-se em mente que apenas dois votos até agora foram proferidos), mas serve como mais um apoio argumentativo de vários outros existentes, justamente pelo fato do processo de globalização na cooperação jurídica probatória internacional, fortalecida pela recente adesão do Brasil à Convenção de Budapeste. Além disso, dadas as constantes superveniências fáticas ao ajuizamento dessas ações, poderão advir alterações, por atos empresariais das próprias *Big Techs,* quanto à tecnologia utilizada na troca de mensagens criptografadas; e, as repercussões de ações de outros países, mediante alianças ou por atos isolados de soberania, especialmente os EUA, sobre o proceder técnico dessas empresas, repercutirão no julgamento dessas demandas, por se tratarem das mesmas questões fáticas (coerência fática-normativa).

De tal modo, ao cabo do presente trabalho, pretende-se realizar uma compilação sistematizada de possibilidades viáveis tecnicamente, alicerçada em dados técnicos, na tentativa da construção de um espaço imparcial que, respeitado o ordenamento jurídico interno de uma Nação, mas com base no direito comparado, embase a nova tecnologia da E2EE a um fim equilibrado à democracia, às garantias constitucionais, mas também, à efetividade na concretização investigativa criminal e da cooperação jurídica internacional sobre provas em matéria penal, algo que se anuncia cada vez mais presente à resolução de casos concretos.

Finalmente, cabem algumas ponderações à metodologia, que ultrapassam a exposição introdutória padrão. É que o esclarecimento de utilização de alguns conceitos jurídicos, desde agora, evitará a multiplicação de explicações a cada nova inserção, ou, ao menos servirão para estancar eventuais interpretações divergentes; por isso, parecem melhor posicionados neste espaço preambular.

---

[9] CONSELHO DA EUROPA. **Convenção sobre o Cibercrime**. Budapeste, 23 nov. 2001. Disponível em: https://rm.coe.int/16802fa428. Acesso em: 19 dez. 2022. Aderida pelo Brasil em dezembro de 2021.

Por primeiro, delimitando-se o ponto principal desta dissertação, como do seu título autoexplicativo, não se deve confundir a interceptação do fluxo das comunicações telemáticas, com aplicação das limitações constitucionais (art. 5º, incisos X e XII, da CF; Lei n. 9296/96)[10], e a quebra de sigilo telemático para mera informação de dados (requisição de dados, ou registros estáticos, pessoais armazenados pelo provedor de internet)[11], com limites legais decisórios distintos[12]. Em segundo lugar, no intuito de resumir as denominações jurídicas em referências à produção de provas penais ilícitas em situações de irregularidade distintas, será utilizado, via de regra, o termo "prova ilícita" em sentido amplo, eliminando a necessidade de que, por reiteradas vezes, diferencie-se se é caso de ofensa a normas de direito material e processual, pois "há dispositivos constitucionais ou legais que têm um aspecto bifronte"[13], como ocorre na interceptação telefônica e telemática. Em terceiro e derradeiro aclaramento, não serão aprofundados aspectos técnicos da informática, mas das conclusões diretas dos especialistas de conceitos e falhas ligados à criptografia e aos meios de investigação criminal de novas tecnologias, em certos momentos importantes para corroborar as teses jurídicas, como é comum nesse tipo de pesquisa.

---

[10] Nesse sentido: "A interceptação de comunicação telemática, portanto, é a obtenção de trocas de mensagens, textos, imagens por aplicativos ou outros serviços de informática, sem o conhecimento dos interlocutores, tendo por objetivo encontrar provas em um processo penal", aplicando-se a Lei n. 9296/96. (In: MOURA, Grégore Moreira de. **Curso de direito penal informático**. Belo Horizonte: D'Plácido, 2021, p. 392-393). Vide, também, o rodapé n. 421.

[11] Na forma dos arts. 10, 21 e 22, todos do Marco Civil da Internet (MCI). Cf.: RMS 60.698/RJ. Relator: Min. Rogério Schietti Cruz, 3ª Seção, julgado em 26/08/2020. **DJe**, 04 set. 2020.

[12] WENDT, Emerson; JORGE, Higor Vinícius Nogueira. **Crimes cibernéticos**: ameaças e procedimentos de investigação. Rio de Janeiro: Brasport. 2013, p. 125.

[13] BADARÓ, Gustavo Henrique. **Epistemologia judiciária e prova penal** [livro eletrônico]. São Paulo: Thomson Reuters Brasil, 2019, p. 142-143.

2 A CRIPTOGRAFIA PONTA A PONTA E A DIFÍCIL PRODUÇÃO DA PROVA PENAL DIGITAL

2.1 CONSIDERAÇÕES INICIAIS QUANTO À CRISE GLOBAL ADVINDA COM A E2EE

A maior dificuldade a ser resolvida na atualidade quanto à produção da prova digital é a manutenção, ou não, da criptografia ponta a ponta, abreviada em muitos trabalhos pelo termo **E2EE**, do inglês "*end-to-end encryption*", pois se refere à possibilidade de leitura somente entre os interlocutores, usuários diretos de cada máquina[14], nos principais meios de comunicação eletrônica.

Importante desde o início destacar, evitando-se indução em erro de interpretação do leitor, que quando se falar em mensagem criptografada ponta a ponta, ela, por si só, segundo todas as bibliografias pesquisadas ao longo deste trabalho, gera a impossibilidade técnica de leitura por terceiros, que não os usuários diretos, pelos meios tecnológicos atuais. A possibilidade de leitura surge somente quando se fala em meios alternativos de espionagem. Por isso, a criptografia ponta a ponta tornou-se um dilema mundial, já que obsta investigações criminais, mesmo que deferida por juízo competente, algo sem precedentes no direito processual penal.

Em suma, o ideal seria a manutenção da criptografia ponta a ponta com a possibilidade de investigação criminal nos aplicativos de mensagens, segurança desenvolvida pelas maiores empresas do mundo para melhor garantia à segurança de seus clientes, até porque sua exclusão é impossível, não pelo motivo de as empresas não conseguirem ou os governos não possam impô-la de alguma maneira, mas porque seria uma utopia diante da facilidade atual de se utilizar de aplicativos que permitem a criptografia, ou, por serviço já prestado para criminosos com tal finalidade.

Assim, mantida a criptografia, estão resguardadas a intimidade, a vida privada, a liberdade de informação e de livre manifestação do pensamento, sem contar aspectos de sigilo econômico nas transações empresariais e monetárias pelo meio digital. Ao mesmo tempo, é possível a investigação criminal de dados

---

[14] A E2EE **"é um método para criptografar comunicações entre destinatário e remetente, de modo que os mesmos sejam as únicas pessoas que podem descriptografar os dados**. Suas origens remontam aos anos 90 [...]." (Cf.: ACADEMY BINANCE. **O que é Criptografia de Ponta a Ponta (E2EE)?** Jul. 2020. Disponível em: https://academy.binance.com/pt/articles/what-is-end-to-end-encryption-e2ee. Acesso em: 30 nov. 2021).

criptografados ponta a ponta, mas somente por soluções ou estratégias policiais alternativas; e daqui advém a expressão "*Going Dark*", usual nos EUA, já que, certamente, muitas das mensagens ficam "às escuras" dos olhos das autoridades.

Portanto, resta dificultada ou obstada boa parte das investigações por razões de ordem técnica, mesmo em governos democráticos e dentro das regras de um devido processo legal, sobretudo aquelas pretendidas fossem interceptadas em tempo real entre interlocutores, tão comuns nas interceptações telefônicas, tecnologia em processo de obsolescência[15] e que, quiçá, desaparecerá. Aqui está a demanda principal de governos e autoridades por todo o mundo: a retirada de parte de seus poderes de Estado por empresas privadas, as consequências à devida persecução penal, sem prejuízo da responsabilidade civil, administrativa e penal das pessoas jurídicas por novas legislações.

Procura-se também, assim, uma solução intermediária, para evitar a concretização da exclusão inútil da criptografia por empresas lícitas e de renome internacional, em nome do resguardo de gama de direitos e garantias constitucionais igualmente relevantes. Talvez a cooperação dessas empresas seja um caminho mais satisfatório que a radicalização nesse novo mundo.

Do entorno técnico do que seria a criptografia ponta a ponta e as mais diferentes visões dos especialistas que tangenciam o tema sobre a (im)possibilidade de sua quebra para a leitura de terceiros, é preciso enfatizar que aquela pode ter aplicação tecnológica distinta em diversos aplicativos de mensagens, como a simétrica ou assimétrica[16], prometendo ser esta inviolável quanto à segurança digital:

> **A criptografia simétrica, não aplicada pelo WhatsApp,** não é tão segura porque a chave precisa estar presente nas duas pontas, o que aumenta as chances dela ser interceptada. **Já a criptografia usada pelo WhatsApp, é um tipo de criptografia assimétrica**: se A deseja enviar uma mensagem para B, vai usar sua chave privada e a chave pública do destinatário; B, por sua vez, irá usar a chave pública do A e sua chave privada para ver o que ele enviou. **O método protege texto, voz, fotos, vídeos, documentos e até ligações** [17]. (Grifo nosso).

---

[15] Nesse mesmo sentido, aduz o autor, delegado de polícia, que a "crescente utilização de smartphones [torna] quase obsoletas as conversas por meio de ligações telefônicas" (p. 134). Cf.: OLIVEIRA, Wagner Martins Carrasco de. Interceptação telefônica e interceptação telemática como meios tecnológicos no combate à corrupção. In: JORGE, Higor Vinicius Nogueira (Coord.). **Enfrentamento da corrupção e investigação criminal tecnológica**. 2. ed. São Paulo: JusPodivm, 2021.

[16] Cf.: GOGONI, Ronaldo. Como funciona a criptografia de ponta a ponta do WhatsApp. **Tecnoblog**, 2019. Disponível em: https://tecnoblog.net/299425/como-funciona-a-criptografia-de-ponta-a-ponta-do-whatsapp. Acesso em: 29 nov. 2021.

[17] *Ibid*.

Ocorre que a velocidade da evolução da tecnologia abarca a possibilidade da quebra dessa criptografia em futuro próximo e, por conseguinte, arquivos digitais são hoje capturados e arquivados para ser burlada a criptografia logo que possível:

> Embora a segurança digital, em 2021, tenha muito o que se preocupar, o governo dos EUA já está pensando em problemas futuros, como a **ascensão de computadores quânticos e a possibilidade deles conseguirem descriptografar dados que estão sendo roubados atualmente**. A estratégia dos criminosos, basicamente, faz com que eles tenham acesso a dados sensíveis de governos, como o dos EUA, no ano atual, mas como não conseguem saber o que está contido nos arquivos por conta da criptografia usada, eles **seguram essas informações até o eventual futuro onde computadores quânticos acessíveis existem**. É por isso que o Departamento de Segurança Interna dos EUA (DHS) e outros órgãos do governo estadunidense estão já planejando formas de enfrentar o cenário da segurança digital em um **mundo pós-criptografia quântica**.[18] (Grifo nosso).

Por tal motivo, cai por terra a alegada total impossibilidade de leitura de dados digitais criptografados ponta a ponta, seja em tempo real, seja futuramente (dados gravados e arquivados), dado o desenvolvimento da computação quântica ou a utilização de outro meio técnico possível mediante alternativas várias, vistas logo à frente.

2.2 O WHATSAPP COMO PARÂMETRO DE ESTUDO E SUAS FALHAS TÉCNICAS: POSSIBILIDADES DE CAPTURA DAS MENSAGENS CRIPTOGRAFADAS

O WhatsApp é o aplicativo mais utilizado no Brasil[19] e possui o maior número de usuários no mundo, tido pelos especialistas por possuir serviço de mensagem digital seguro, pois dotado da criptografia ponta a ponta. O gráfico a seguir, atualizado em outubro de 2021, mostra, em milhões[20], os aplicativos mais utilizados no globo.

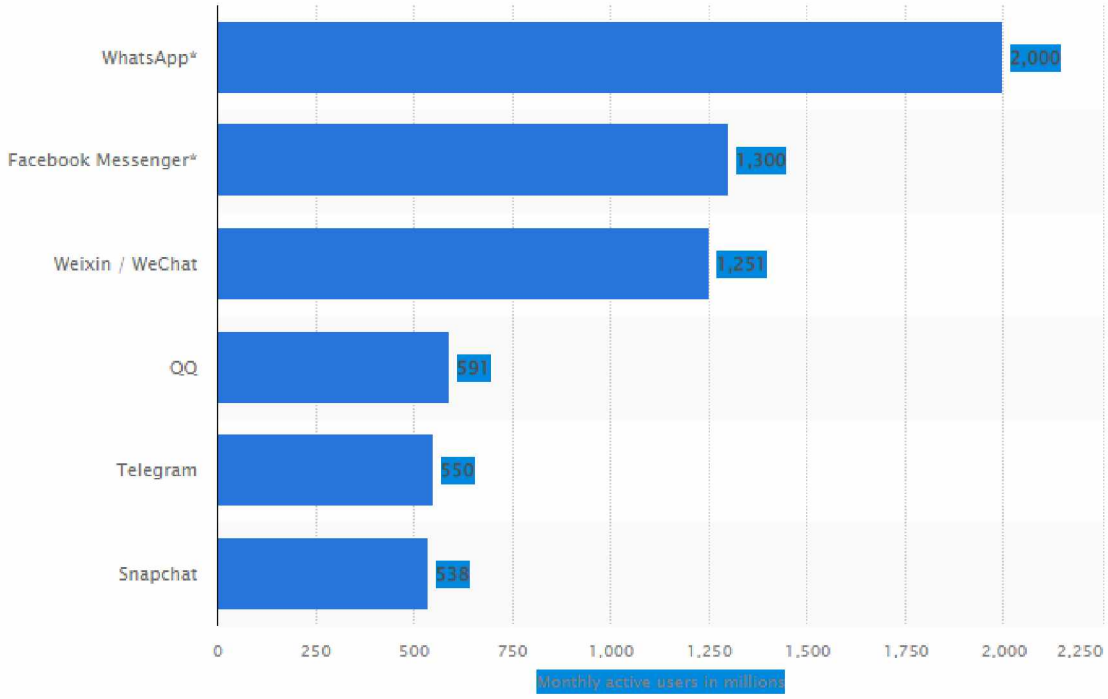
GRÁFICO 1 – Most popular global mobile messaging Apps 2021

---

[18] In: BRANCO, Dácio Castelo. Criptografia pós-quântica? EUA investem em segurança de dados mais eficaz. **Canaltech**, 4 nov. 2021. Disponível em: https://canaltech.com.br/seguranca/criptografia-pos-quantica-eua-investem-em-seguranca-de-dados-mais-eficaz-200842. Acesso em: 02 nov. 2021.

[19] Cf. ARBULU, Rafael. WhatsApp é o app mais usado por brasileiros. **Olhar Digital**, 21 dez. 2020. Disponível em: bit.ly/3vgFHU2. Acesso em: 29 nov. 2021).

[20] STATISTA RESEARCH DEPARTMENT. **MOST popular global mobile messenger apps as of October 2021, based on number of monthly active users**. Nov. 2021. Disponível em: https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-app. Acesso em: 29 nov. 2021.

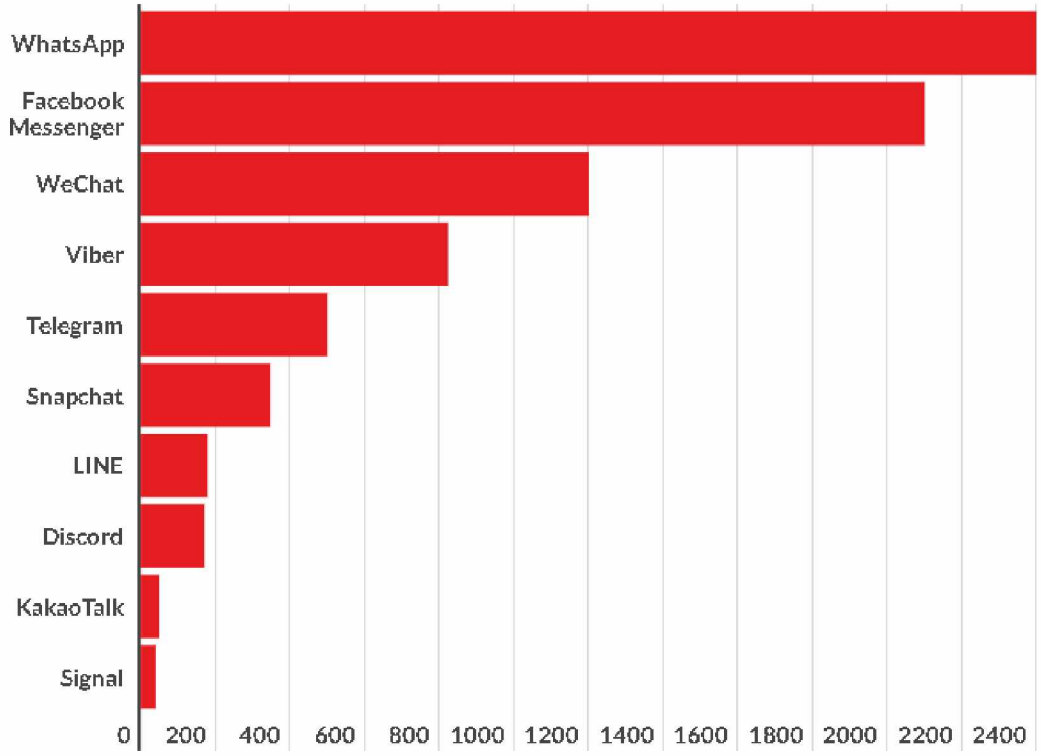


Fonte: Statista Research Department (2021).

E, por informações atualizadas até 13 de setembro de 2022[21], o WhatsApp não só permanece na primeira colocação, como até aumentou o número de usuários, conforme gráfico a seguir (em bilhões):

GRÁFICO 2 – *Messaging Users by App 2022* (*bn*)

[21] CURRY, David. Messaging App Revenue and Usage Statistics (2022). **Business of Apps**, 13. Sep. 2022. Disponível em: https://www.businessofapps.com/data/messaging-app-market/#:~:text=WhatsApp%20is%20the%20most%20popular%20messaging%20app%20worldwide%2C%20and%20is,Middle%20East%20and%20South%20America. Acesso em: 07 nov. 2022.



FONTE: Company Data, TechCrunch (*apud* CURRY, 2022)

Surpreende, também, a cifra de mensagens diárias entregues (em 2020): mais de 100 bilhões[22], do qual ainda se estende um efeito multiplicador ao WhatsApp. É que, ao cadastrar o usuário através de seu número de telefone, o *software* passa a ter acesso a toda a agenda de seus contatos disponíveis no aparelho celular[23], certamente, mais um diferencial no aspecto relativo à interpretação do conceito de privacidade para fins de aplicação do art. 5º, XII, da CF.

Em face do elevado número de usuários e de mensagens do WhatsApp, sem esquecer-se de pertencer ao Facebook (incorporado à nova empresa "*Meta*")[24], o qual promete incorporar a criptografia ponta a ponta em mensagens de outros aplicativos (como o Instagram e o Facebook Messenger[25]), ou seja, atingindo ainda mais de um

---

[22] NOGUEIRA, Luiz. WhatsApp revela que agora entrega 100 bilhões de mensagens por dia. **Olhar Digital**, 30 out. 2020. Disponível em: https://olhardigital.com.br/2020/10/30/noticias/whatsapp-agora-entrega-cerca-de-100-bilhoes-de-mensagens-por-dia. Acesso em: 2 dez. 2021.

[23] LEMOS, Bruno Espiñeira; QUINTIERI, Victor Minervino. **Técnicas especiais de investigação no processo penal**. Belo Horizonte: D'Plácido, 2017, p. 101.

[24] Informações constantes no aplicativo WhatsApp. Cf.: META. Disponível em: https://about.facebook.com/br/company-info. Acesso em: 29 nov. 2021.

[25] Contraditoriamente, por evidente pressão política ao Facebook, apesar de já existir a E2EE, a Meta recuou na sua implantação ao Messenger, justamente em face das novas propostas legislativas nos Estados Unidos quanto à restrição da criptografia para investigação criminal, já indicando maneiras de monitoramento sem retirar o sigilo necessário à privacidade de seus usuários.

bilhão de usuários[26], pertinente trazer informações básicas do funcionamento do aplicativo de mensageria líder brasileiro e mundial para atingir o conceito de criptografia ponta a ponta trazida no *site* do próprio WhatsApp, para a proteção de "mensagens, fotos, vídeos, mensagens de voz, atualizações de status, documentos e chamadas"[27]:

> A criptografia de ponta a ponta garante que somente você e a pessoa com quem você está se comunicando podem ler ou ouvir as mensagens trocadas. Ninguém mais terá acesso a elas, nem mesmo o WhatsApp. Suas mensagens estão seguras com cadeados e somente você e a pessoa com quem você está se comunicando possuem as chaves especiais necessárias para destrancá-los e ler suas mensagens. Todo esse processo acontece automaticamente: não é necessário ativar configurações ou estabelecer conversas secretas especiais para garantir a segurança de suas mensagens.
> [...]
> Além disso, **as chaves mudam com cada mensagem que é enviada**.

Ademais, recentemente[28], o WhatsApp passou a estender a opção de criptografia ponta a ponta também ao *backup* das conversas, antes uma brecha para as autoridades investigativas: "Com o *backup* criptografado de ponta a ponta, você pode adicionar essa mesma camada de proteção a *backups* salvos no iCloud ou no Google Drive".[29]

A criptografia ponta a ponta se estende aos grupos de mensagens formados no WhatsApp[30], maneira comum de comunicação de organizações criminosas. Mas,

---

[26] A Meta não pretende implementar a E2EE no Messenger e no Instagram até 2023, sem antes implantar **meios alternativos** de proteção para evitar crimes sexuais" (Grifo nosso. Cf.: ALMENARA, Igor. Facebook Messenger e Instagram só terão criptografia de ponta a ponta em 2023. **Canaltech**, 23 nov. 2021. Disponível em: https://canaltech.com.br/redes-sociais/facebook-e-instagram-so-terao-criptografia-de-ponta-a-ponta-em-2023-202585. Acesso em: 29 nov. 2021).

[27] WHATSAPP. **Sobre a criptografia de ponta a ponta**. 2021. Disponível em: https://faq.whatsapp.com/general/security-and-privacy/end-to-end-encryption/?lang=pt_br. Acesso em: 30 nov. 2021.

[28] A partir de 14 out. 2021. LOUBAK, Ana Letícia. **WhatsApp agora tem opção para criptografar backup de conversas; entenda**. **Techtudo**, 10 out. 2021. Disponível: https://www.techtudo.com.br/noticias/2021/10/whatsapp-agora-tem-opcao-para-criptografar-backup-de-conversas-entenda.ghtml. Acesso em: 30 nov. 2021.

[29] WHATSAPP. **Sobre o backup criptografado de ponta a ponta**. Disponível em: https://faq.whatsapp.com/general/chats/about-end-to-end-encrypted-backup/?lang=pt_br. Acesso em: 30 nov. 2021.

[30] CASELLI, Guilherme. **Manual de Investigação Criminal**. São Paulo: JusPodivm. 2021, p. 286: "No caso específico de conversas em grupo, foi verificado que o servidor do WhatsApp tem a capacidade de influenciar no gerenciamento do grupo (e.g., **adicionando usuários sem que haja uma ação dos administradores do grupo pedindo tal inclusão**)" (Grifo nosso).

justamente em grupos de mensagens de WhatsApp provou-se falhas de segurança apontadas em relatório de importante Simpósio europeu de 2018[31]:

> Os pontos fracos descritos habilitam o invasor A, que controla o servidor WhatsApp ou pode quebrar o transporte da camada de segurança, para **assumir o controle total sobre um grupo**. Entrando no grupo, no entanto, **deixa rastros**, uma vez que esta operação está listada na interface gráfica do usuário. O **servidor WhatsApp pode, portanto, usar o fato de que ele pode reordenar furtivamente e soltar mensagens no grupo**. Assim, ele pode enviar um cache de mensagens para o grupo, ler o conteúdo primeiro e decidir a ordem em que são entregues aos membros. Além disso o servidor WhatsApp pode encaminhar essas mensagens para os membros individualmente, de modo que uma combinação sutilmente escolhida de mensagens pode ajudá-lo a cobrir os rastros (p. 11; tradução e grifo nossos).

Essa falha em conversas em grupos de WhatsApp mostrou alteração do verdadeiro remetente da mensagem[32] e até de seu texto, expondo fato gravíssimo, que poderia alterar todo o conjunto probatório em eventual julgamento:

> Ao converter o protocolo em Json, o grupo foi capaz de entender a forma como ele trabalhava e assim, fazer os seguintes movimentos invasivos: 1. Usar o recurso de citação em uma conversa em grupo para **alterar a identidade do remetente, mesmo que essa pessoa não seja um membro do grupo. 2. Alterar o texto da resposta de outra pessoa;** 3. Enviar uma mensagem privada para outro participante do grupo, tirando assim a preocupação de estar se falando num grupo, porém, a conversa é enviada a todos os usuários inclusos naquele grupo. [33] (Grifo nosso).

Já houve notícia de falha na criptografia ponta a ponta do WhatsApp[34] nestas hipóteses: a) ao se fazer uso de um *spyware* denominado Pegasus[35]; b) e no uso da ferramenta do WhatsApp Web, esta evidenciada em face de seu uso pela Alemanha

---

[31] Cf.: ROSLER, Paul; MAINKA, Christian; SCHWENK, Jörg. More is Less: On the End-to-End Security of Group Chats in Signal, WhatsApp, and Threema. In: IEEE EUROPEAN SYMPOSIUM ON SECURITY AND PRIVACY, 3rd, 2018, London. **Proceedings...** London: EuroS&P, 2018. Disponível em: https://eprint.iacr.org/2017/713.pdf. Acesso em: 30 nov. 2021.

[32] Sobre os pilares de uma comunicação digital segura e as formas técnicas de verificação da sua autoria e de que seu conteúdo não foi modificado, como o resumo de mensagem (número de *hash*), vide: BARRETO, Alesandro Gonçalves; KUFA, Karina; SILVA, Marcelo Mesquita. **Cibercrimes e seus reflexos no direito brasileiro**. 2. ed. São Paulo: JusPodivm, 2021.

[33] TUDO CELULAR. **WhatsApp tem falha de criptografia que permite manipulação de conversas descoberta**. 2018. Disponível em: https://www.tudocelular.com/seguranca/noticias/n128932/whatsapp-vulnerabilidade-criptografia-descoberta.html. Acesso em: 30 nov. 2021.

[34] MANCUSO, Ronnie. A criptografia do WhatsApp foi furada? Fato ou mito? **Olhar Digital**, 9 set. 2021. Disponível em: https://olhardigital.com.br/2021/09/09/seguranca/a-criptografia-do-whatsapp-foi-furada-fato-ou-mito. Acesso em: 28 out. 2021.

[35] NOGUEIRA, Luiz. Criptografia de ponta a ponta do WhatsApp não é infalível. **Olhar Digital**, 4 nov. 2019. Disponível em: https://olhardigital.com.br/2019/11/04/noticias/criptografia-de-ponta-a-ponta-do-whatsapp-nao-e-infalivel. Acesso em: 30 nov. 2021.

como tática investigativa criminal e já tratada em julgados no Colendo STJ, como se verá, oportunamente, nesta dissertação[36]:

> [há] brecha de segurança crítica no WhatsApp Web [...]. O problema afeta também as versões desktop e o app para a Windows Store. [...] **atacantes podem ter acesso a mensagens, fotos e conteúdos compartilhados no WhatsApp.** Com isso, **hackers podem se passar por usuários** para conseguir vantagens ou aplicar golpes. "Essa vulnerabilidade, além de poder ser explorada de uma maneira muito simples, tem uma **rastreabilidade praticamente inexistente**". [37] (Grifo nosso).

Esses breves relatos de falhas em mensagens dotadas de criptografia ponta a ponta corroboram a possibilidade de burla, por criminosos e pelo Estado, como divulgado, recentemente, em documento do FBI[38].

De uma forma global, contudo, a E2EE, de fato, gera maior segurança aos seus usuários. Constantes avanços das empresas de mensageria digital equivalentes corroboram que este acesso, sem se utilizar de falhas pontuais no sistema de criptografia, é muito difícil para os órgãos de persecução penal, inclusive dentro do próprio Estados Unidos, como se infere de precedentes judiciais e do *site* do WhatsApp.

Dessas diretrizes no *site* do WhatsApp, há informação de que se divulgam apenas **registros** das contas (não armazena mensagens), de acordo com a lei federal norte-americana denominada *Stored Communications Act*[39], em investigações criminais oficiais, após mandado judicial de busca, deixando claro que estão excluídos os conteúdos das comunicações, pois a E2EE está sempre ativada. E, sobre os requisitos legais de processos internacionais, frisa um juízo de valor realizado pela empresa, que pode ser interpretado como um indicativo de sua responsabilização jurídica:

> [...] **avaliaremos se as solicitações seguem padrões reconhecidos internacionalmente, como leis de direitos humanos, devidos processos legais e o domínio da lei. Pode ser necessário um Tratado de assistência**

---

[36] Vide o subcapítulo 3.3.

[37] BRANDÃO, Hemerson. Empresa alerta sobre grave falha de segurança no WhatsApp Web. **Minha Operadora**, jul. 2021. Disponível em: https://www.minhaoperadora.com.br/2021/07/empresa-alerta-sobre-grave-falha-de-seguranca-no-whatsapp-web.html. Acesso em: 30 nov. 2021.

[38] PETROV, Daniel. FBI encrypted chat access scorecard ranks iMessage and WhatsApp easy, Telegram hard. **Phone Arena**, 2 dez. 2021. Disponível em: https://www.phonearena.com/news/fbi-encrypted-chat-access-imessage-whatsapp-signal-telegram_id136809. Acesso em: 2 dez. 2021.

[39] A respeito, vide o capítulo 3.1.4.

> **recíproca ou uma carta rogatória** para forçar a divulgação do conteúdo de uma conta. [40] (Grifo nosso).

Como destaque último de incessantes alterações da tecnologia, em entrevista realizada do *site* UOL (Tilt) com Pablo Bello[41], diretor de políticas públicas do WhatsApp na América Latina, surgiu a informação da possível rastreabilidade dos usuários (registro de quando alguém usou o aplicativo, com quem conversou, de quem recebeu, para quem enviou ou reenviou alguma mensagem), já visando eventual cumprimento do Projeto de Lei n. 2.630/20 (conhecia por "Lei das Fake News")[42]:

> **Não é que seja impossível fazer modificações para adotar a rastreabilidade.** Consideramos a solução ruim e inadequada para os brasileiros e para o mundo. **Nós nos opomos, não porque tecnologicamente não se pode fazer, mas porque é uma solução que rompe com o princípio da privacidade dos usuários**. Ela é um presente para regimes autoritários, afeta jornalistas, ativistas de direitos humanos e põe em risco pessoas inocentes. É ruim inclusive para a liberdade de expressão (Grifo nosso).

Em síntese, existem falhas graves mesmo nos aplicativos que prometem segurança nas mensagens entre usuários através da criptografia ponta a ponta. Por outro lado, fica evidente que são casos isolados decorrentes de ordem técnica do próprio sistema, ou, provocada por um terceiro (*spyware*), não por ato voluntário da empresa. Há, ainda, outras maneiras de investigação criminal, mas Estados relatam enormes dificuldades de realizar a interceptação telemática de forma usual, como na telefônica, mesmo presente ordem judicial motivada e dentro do devido processo legal. E demonstradas as dificuldades técnicas à atividade investigativa criminal para o acesso a tais provas digitais, além da divergência entre os diversos interessados, decorre toda a discussão jurídica ora em análise. Resta saber se cabível uma solução intermediária e se alguma parte cederá.

---

[40] Cf.: WHATSAPP. **Informações para as autoridades policiais**. Disponível em: https://faq.whatsapp.com/general/security-and-privacy/information-for-law-enforcement-authorities. Acesso em: 30 out. 2022.

[41] Cf.: GOMES, Helton Simões. WhatsApp: "PL para rastrear mensagem classifica todos como suspeitos". **UOL**, São Paulo, 23 jul. 2020. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/06/23/rastrear-mensagem-e-por-tornozeleira-eletronica-em-usuario-diz-whatsapp.htm. Acesso em: 08 ago. 2021).

[42] A proposta não trata da quebra da E2EE, só do dever de guarda de "registros dos envios das mensagens", resguardando a privacidade quanto ao conteúdo, sob pena de sanções administrativas (arts. 10, 30 e 31 – ver: BRASIL. Câmara dos Deputados. Projeto de Lei n. 2630/2020. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1909983&filename=PL+2630/2020. Acesso em: 25 nov. 2022).

A divergência técnica acima indicada, além da possibilidade de estar contaminada por fatores diversos (v.g. econômico, político, jurídico e cultural de diversos países em casos como da E2EE) repercute, em diversos processos judiciais já realizados, na utilização pelo juízo em sua motivação da teoria da ponderação de Robert Alexy, especialmente em face das novas tecnologias da era digital. Mas, para a concretização dessa teoria, há reticente aplicabilidade quando o julgador depende de perícias, devendo-se adequá-la para a melhor forma possível a um julgamento justo, evitando-se premissas falsas ao julgador.

Há estudo aprofundado do *Berkman Center for Internet & Society at Harvard University*, o qual procurou expor de forma técnica (e, ao menos do que se interpretou, imparcial) uma série de informações sobre a E2EE, em especial, a possibilidade de uso dos metadados na interceptação telemática em tempo real, algo inexplorado em todas as outras pesquisas. Com isso, acaba-se revelando que uma perícia completa e atual é ponto essencial da correta valoração do debate e decisão judicial sobre o tema:

> A **criptografia ponta a ponta e outras arquiteturas tecnológicas para obscurecer os dados do usuário são improváveis de serem adotadas de forma onipresente pelas empresas** [...]; As **imagens estáticas, vídeo e áudio** capturados por esses dispositivos podem permitir a interceptação e gravação **em tempo real** com acesso **após os fatos** [...] por meio de um canal diferente; Os **metadados não são criptografados** e a grande maioria provavelmente permanecerá assim. Estes **são dados que precisam permanecer descriptografados** para que os sistemas operem: dados de localização de celulares e outros dispositivos, registros de chamadas telefônicas, informações de cabeçalho em e-mail [...].[43] (tradução e grifo nossos).

As ações constitucionais na Suprema Corte brasileira, que oportunamente serão abordadas neste trabalho[44], evidenciam esta peculiaridade quanto às perícias, tanto que, em audiências públicas realizadas[45], observaram-se, daquilo que poderia ser um ponto de vista técnico, "verdades" diversas trazidas pelos especialistas, os quais acabaram sequer repercutindo na motivação dos votos, até agora proferidos, de

---

[43] Cf.: DELONG, Johnet al. **Don't Panic Making Progress on the "Going Dark" Debate**. Cambridge: Berkman, 2016. Disponível em: https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf. Acesso em: 16 nov. 2021. p. 7.

[44] Vide o subcapítulo 4.2.

[45] BRASIL. Supremo Tribunal Federal. **Audiência pública - Bloqueio judicial do WhatsApp e Marco Civil da Internet (1/4).** Disponível em: https://www.youtube.com/watch?v=3TNsQCNIOO0. Acesso em: 06 nov. 2022.

forma incisiva, dada a divergência quanto à possibilidade ou não da quebra da E2EE, ou, de possibilidades alternativas à investigação criminal.

Nos EUA, a sua Suprema Corte delineou as linhas de raciocínio quanto à obediência da cadeia de custódia em perícias ligadas às novas tecnologias, as quais, apesar de aplicáveis ao Brasil quanto à tal forma, já há críticas da doutrina norte-americana sobre sua concretização processual no que tange ao conteúdo probatório:

> Com o **aprimoramento e a popularização da tecnologia**, **os peritos técnicos passaram a ser utilizados com mais frequência pelos tribunais** e, desde então, o direito busca soluções processuais para lidar com esse tipo de evidência. No caso Daubert v. Merrell Dow Pharmaceuticals, que se tornou paradigmático nos Estados Unidos em 1993, a Suprema Corte determinou (p. 161) [...] cinco fatores: se a teoria ou técnica em questão pode ser ou foi testada; se ela foi submetida a peer review e publicação; sua margem de erro; a existência e manutenção de padrões de controle sobre a operação; se ela é amplamente aceita na comunidade científica relevante (FELDMAN, 2001, p. 2-3). Não raramente, todavia, os tomadores de decisão norte-americanos expressam dificuldades em avaliar esses parâmetros (DWYER, 2008, p. 2), o que poderia indicar que **a mera regulação formal de critérios legais não é suficiente** para permitir a transposição dos argumentos científicos para o sistema jurídico com clareza e previsibilidade. Além disso, os critérios formalizados servem para auxiliar o tomador de decisões quanto à **admissibilidade dos peritos**, **mas permanece a dificuldade para avaliar a qualidade dos argumentos técnico-científicos** e, consequentemente, **a dificuldade de acessar, através da fórmula do peso, a confiabilidade das premissas empíricas apresentadas** (p. 164).[46] (Grifo nosso).

Com todas essas problemáticas expostas, no próximo subcapítulo, necessária a sistematização dos argumentos tanto daqueles que (1) defendem a manutenção da criptografia ponta a ponta tal como já está, de forma absoluta, refutando qualquer possibilidade técnica de leitura durante ou depois da troca de mensagens entre os interlocutores, ou, (2) dos que almejam uma possibilidade técnica contrária (v.g. o *hacking* do Estado através de um cavalo de Troia, ou outros meios); aqui, em tese, dentro do estado democrático de direito e voltado ao combate da criminalidade e ao resguardo dos direitos das vítimas, aliás, prerrogativas, em tese, tão legítimas[47] quanto dos que lutam pelos direitos e garantias fundamentais da privacidade, liberdade de expressão e de pensamento.

---

[46] Cf.: OLIVEIRA, Ana Carolina Rezende. Direito, ciência e a racionalidade das premissas empíricas na fórmula do peso de Robert Alexy. In: MARCO, Cristhian Magnus de; BELOTTO, Julian Cristopher; GUSBERTI, Anderson Rodrigo (Org.). **Direitos fundamentais na perspectiva teórica de Robert Alexy**: Tomo VI. Joaçaba: Unoesc, 2016. (Série Direitos Fundamentais Civis), p. 161 e 164.

[47] A falta de protagonismo da vítima no Direito Penal e Processual Penal é evidente, daí o uso do termo "neutralização da vítima" (Cf.: HASSEMER, Winfried. Introdução aos Fundamentos do Direito Penal. Tradução: Pablo Rodrigo Alflen da Silva. Porto Alegre: Sergio Antonio Fabris, 2005, p. 118 e 124), ou, "expropriação do conflito" (e ainda: OBARRIO, María Carolina; QUINTANA, María. **Mediación Penal**. Buenos Aires: Editorial Quorum, 2004, p. 20; tradução nossa).

2.3 DELIMITAÇÕES DO EMBATE MUNDIAL ENTRE AS *BIG TECHS* E NAÇÕES PODEROSAS PELA QUEBRA DA E2EE EM NOME DA INVESTIGAÇÃO CRIMINAL

As novas tecnologias de comunicação via *internet* geraram uma crise global quanto à efetividade da persecução penal. Exemplo disso foram os inúmeros casos de bloqueio do uso do *WhatsApp* no Brasil, após ordem judicial, que culminaram em comoção nacional e desbloqueio pela Suprema Corte – aliás, objeto de ações constitucionais, ainda em andamento, na ADPF 403, relator Min. Edson Fachin, e ADI 5527, de relatoria da Min. Rosa Weber[48], as quais serão objeto de estudo em capítulo próprio desta dissertação. Mas, adianta-se, revelam tais demandas que a criptografia ponta a ponta acrescentou mais esta dificuldade na investigação criminal em vários aplicativos de mensagens digitais, não só no Brasil, mas por todo o mundo. O conflito de garantias e direitos constitucionais[49] (basicamente, segurança pública *versus* privacidade[50] e liberdade da manifestação do pensamento) é o cerne de todo o imbróglio entre seus principais personagens (governos e setor privado, basicamente), o qual, desde já se destaca, tem imposição prática efetiva dificultada pela transnacionalidade das empresas detentoras dessa tecnologia e a normativa diversa de cada país. Sobre o tema, ressaltam-se recentes estudos e julgamentos por todo o mundo, demonstrando sua complexidade, ausente qualquer possibilidade de se antever solução no curto prazo.

Por isso, as formas de como adequar as novas tecnologias à persecução criminal, sem ofensa à Constituição Federal de cada país, é desafio que já está presente no dia a dia da sociedade globalizada. De um lado, com razão, defende-se

---

[48] Vide: STF, ADPF 403 (BRASIL. Supremo Tribunal Federal. **ADPF 403/SE**. Min. Edson Fachin) e ADI 5527 (BRASIL. Supremo Tribunal Federal. **ADI 5527/DF**. Relatora: Min. Rosa Weber).

[49] Na ADPF 403 do STF, quanto à criptografia utilizada no WhatsApp, foi aplicada na motivação do MM. Relator a teoria da ponderação de Robert Alexy, porém, objeções a seu uso merecem alerta, Cf.: **a)** TROIS NETO, Paulo M. C. Têmis no Divã: Fatores Irracionais na ponderação constitucional? In: MARCO, Cristhian M. de; BELOTTO, Julian. C.; GUSBERTI, Anderson. R. (Org.). **Direitos fundamentais na perspectiva teórica de Robert Alexy**: Tomo VI. Joaçaba: Unoesc, 2016. (Série Direitos Fundamentais Civis); **b)** MORAIS, Fausto Santos de. **Ponderação e arbitrariedade**: a inadequada recepção de Alexy pelo STF. Salvador: Juspodivm, 2010; **c)** POSCHER, R. Resuscitation of a Phantom? On Robert Alexy's Latest Attempt to Save His Concept of Principle. **Ratio Juris**, v. 33, n. 2, p. 134-149, jul. 2020.

[50] Obviamente, em contrapartida, há limites para tal "privacidade", daí a celeuma do tema.

que quebrar a criptografia, mediante chave secreta para acesso disponibilizada a órgãos competentes (*backdoors*)[51] na comunicação entre particulares geraria instabilidade (vulnerabilidade) na segurança privada de todo o sistema de seus demais usuários não investigados, com graves repercussões, inclusive, econômicas, dado o fluxo de negócios em tais meios, e, de segurança nacional, em face da redução indireta que a criação de *backdoors* pelas empresas de tecnologia para quebra da criptografia em nome da persecução penal geraria na comunicação digital como um todo[52]. Por outro olhar, também com argumentos robustos, defende-se que o uso criminoso de tecnologia, que obsta a investigação criminal, gera impunidade e insegurança pública, agravada pela falta de prova cabal (auditoria independente, imparcial) pelas *Big Techs* de alternativa viável e proporcional para vencer tal desafio em prol do combate a crimes graves e que justificam a interceptação telemática por decisão judicial.

Do já citado estudo de Harvard (2016)[53], extraem-se depoimentos preocupantes, que não podem ser esquecidos, para a busca de uma solução ao problema da E2EE em situações de interesse nacional[54]:

> De acordo com funcionários do governo, o uso de criptografia pode inibir a capacidade da aplicação da lei e a comunidade de inteligência para investigar e prevenir **ataques terroristas**. [...] na Síria estão "recrutando e encarregando dezenas de americanos problemáticos para matar pessoas, [usando] um processo que participa **cada vez mais por meio de aplicativos de mensagens móveis de ponta a ponta criptografadas, comunicações que não podem ser interceptadas, apesar das ordens judiciais ao abrigo da Quarta Emenda**' Funcionários do FBI também enfatizaram que **o FBI não possui a capacidade de derrotar criptografia** [...]". (Tradução e grifo nossos).

Ademais, oportuna a discussão se cabe ao Estado impor, alternativamente, a criação de tais meios por empresas privadas detentoras da tecnologia da criptografia na comunicação, ou se restaria ao Estado, tão somente, a criação de *softwares* ou formas de investigação outras (como está ocorrendo na Alemanha), num jogo não só

---

[51] Conceito: "Um backdoor de criptografia é uma técnica na qual um mecanismo de segurança do sistema é contornado indetectavelmente para acessar um computador ou seus dados" (tradução nossa) – Cf.: ENCRYPTION Backdoor. **Techopedia**, fev. 2020. Disponível em: https://www.techopedia.com/definition/3743/encryption-backdoor. Acesso em: 30 out. 2021.

[52] Estudo robusto sobre *backdoors* em: VOJTKO, Mark. All About Encryption Backdoors. **The SSL Store**, 18 jan. 2021. Disponível em: https://www.thesslstore.com/blog/all-about-encryption-backdoors. Acesso em: 30 out. 2021.

[53] Rodapé n. 43.

[54] Cf.: DELONG, John et al. *Op. cit*, p. 6.

jurisdicional (no Brasil, em julgamento no STF), mas sobretudo político na maioria dos países, nos quais ainda não há debate em suas respectivas Cortes judiciais da análise de conflito de princípios e garantias constitucionais, como no caso brasileiro.

O Poder Legislativo de países como os Estados Unidos[55] e a Alemanha[56] já iniciaram, profundamente, o enfrentamento da matéria sob a premissa de se combater atos de terrorismo e outros crimes gravíssimos (como os crimes sexuais contra crianças). No Brasil, as decisões judiciais acerca da prova obtida em tais fluxos de comunicação criptografada devem se basear numa leitura sistemática de diversas leis, além da óbvia interpretação constitucional à prática investigativa realizada na produção da prova, sem olvidar-se dos problemas de sua admissibilidade como prova lícita e da necessária obediência à cadeia de custódia para legitimar o direito ao contraditório pelo acusado.

Uma análise global objetiva seria unificar regras, princípios e formas de uma produção lícita de provas e, consequentemente, evitar a ineficiência estatal quanto ao poder punitivo em todas as suas frentes (autoridade policial, Ministério Público e Poder Judiciário), porquanto já se verificam no Brasil a declaração de nulidades processuais ante a ausência de uma regulamentação clara ao devido processo legal, como será detalhado adiante em subcapítulo próprio.

A obtenção de lições internacionais para igual fim, já que o tema envolve situações semelhantes em virtude da universalização desses meios de comunicação, é inerente ao presente estudo. Não são poucos os dados e opiniões para ambos os lados: a) a **proibição utópica** da criptografia ponta a ponta, como anteriormente delineado, pois já há serviços de criminosos de venda de celulares dotados de aplicativos criptografados ponta a ponta; b) a sua **manutenção** radicalmente **intocável**[57], afastada qualquer intervenção estatal, já descartada por diversos países democráticos, por declaração governamental, atos de investigação policial e legislação vigente e em tramitação; c) **manter** a E2EE, mas, mediante a criação de

---

[55] Vide o subcapítulo 3.1.5.

[56] Conforme o subcapítulo 3.3.

[57] PFEFFERKORN, Riana. There's now na even worse anti-encryption bill than Earn It. That doesn't make the Earn It bill ok. **CIS**, 24 jun. 2020. Disponível em: https://cyberlaw.stanford.edu/blog/2020/06/there%E2%80%99s-now-even-worse-anti-encryption-bill-earn-it-doesn%E2%80%99t-make-earn-it-bill-ok. Acesso em: 28 nov. 2021. A autora é pesquisadora da Stanford Law School e defende a E2EE.

***backdoors*[58], *hacking* estatal[59] e outros meios estratégicos (v.g.: infiltração, penetração, *man-in-the-midle*, ou, a própria busca e apreensão física do aparelho celular)** para os órgãos de segurança pública[60], que parece ser a tendência possível e útil como opção adaptada à tecnologia vigente. Em síntese, calha a exposição de tais técnicas de investigação digital[61]:

> [...] **há várias formas de as autoridades darem a volta em torno da criptografia de ponta a ponta para acessar os dados e as comunicações de seus usuários**. Isso inclui **backups**, **com informações salvas na nuvem e no Google Drive**, por exemplo; **intimação**, que é o ato de requerer informações [não criptografadas] das próprias empresas, sem a necessidade de que elas acessem o telefone; **"infiltração"**, quando autoridades podem monitorar assuntos ao conseguirem se infiltrar em grupos de conversas ou em canais; e a **penetração**, que é hackear um laptot, já que WhatsApp e Telegram também podem ser acessados pela web. [...] Se as autoridades têm uma ordem judicial, podem conduzir uma vigilância convencional monitorando os suspeitos. Com a **criptografia de ponta a ponta** que alguns aplicativos usam agora, a Polícia Federal obviamente sai em desvantagem. **Apesar de o WhatsApp e o Telegram disporem dessa criptografia, essas mídias sociais podem ser hackeadas, mas sem a necessidade da quebra da criptografia. Hackers e autoridades podem acessar o conteúdo,** porque o WhatsApp e o Telegram dependem de linhas telefônicas, que por sua vez dependem de protocolos (SS7), que podem ser compelidos a revelar dados. **Especialistas de inteligência, autoridades judiciais e hackers podem criar um vírus malware, que, ao grampear uma linha telefônica, clona o aparelho do alvo e permite que o invasor tenha acesso ao celular copiado.** Obviamente, esse tipo de interceptação de dados é conduzido sem

---

[58] Os "***backdoors*** podem já estar instalados previamente no aplicativo [...] utilizado pelas vítimas; [são] 'portas secretas' para um local guardado". Já os ***trojans* ou cavalos de troia** são malwares que têm passagem permitida nos [...] dispositivos dos usuários" (Cf.: JULIO, Clara. Malware backdoor: entenda esse tipo de ameaça e saiba como evitar. **Backup Garantido**, 19 jan. 2021. Disponível em: https://backupgarantido.com.br/blog/malware-backdoor. Acesso em: 03 dez. 2021).

[59] Sobre o ***hacking***, inclusive **pelo Estado**, vide: MALWAREBYTES. **Tudo sobre hacking**. Disponível em: https://br.malwarebytes.com/hacker. Acesso em: 03 dez. 2021. Em destaque: "[...] os hackers também podem usar psicologia para induzir o usuário a clicar em um anexo malicioso ou fornecer dados pessoais. [a chamada] **'engenharia social'**. (*Ibid.*).

[60] As possibilidades são gigantescas e demandaria estudo específico e aprofundado; assim, propõe-se a mera citação das seguintes referências, além das demais exploradas ao longo deste estudo: **a)** RPEK, Lucas. How the FBI Is Trying to Break Encryption Without Actually Breaking Encryption. **Gizmodo**, 18 jun. 2021. Disponível em: https://gizmodo.com/how-the-fbi-is-trying-to-break-encryption-without-actua-1847054471/amp. Acesso em: 01 dez. 2021; **b)** MULLIN, Joe. The FBI Should Stop Attacking Encryption and Tell Congress About All the Encrypted Phones It's Already Hacking Into. **EFF**, 8 mar. 2021. Disponível em: https://www.eff.org/deeplinks/2021/03/fbi-should-stop-attacking-encryption-and-tell-congress-about-all-encrypted-phones. Acesso em: 01 dez. 2021; **c)** NICAS, Jack. Bitcoin and Encryption: A Race Between Criminals and the F.B.I. **The New York Times**, 12 jun. 2021. Disponível em: https://www.nytimes.com/2021/06/12/technology/fbi-bitcoin-ransom-encryption.html. Acesso em: 01 dez. 2021; **d)** RILEY, Tonya. The Cybersecurity 202: FBI renews attack on encryption ahead of another possible attack on the Capitol. **The Washington Post**, 4 mar. 2021. Disponível em: https://www.washingtonpost.com/politics/2021/03/04/cybersecurity-202-fbi-renews-attack-encryption-ahead-another-possible-attack-capitol. Acesso em: 01 dez. 2021.

[61] Cf.: SOPRANA, Paula. Como a polícia pode dar a volta na criptografia do WhatsApp. **Época**, 23 jul. 2016. Disponível em: https://epoca.globo.com/vida/experiencias-digitais/noticia/2016/07/como-policia-pode-dar-volta-na-criptografia-do-whatsapp.html. Acesso em: 12 out. 2021.

> o consentimento do usuário e viola sua privacidade. [...] Também há o **hacking de Estado**, embora eu não seja uma apoiadora.

Outras duas técnicas possíveis para a interceptação telemática através de aplicativos como o WhatsApp em auxílio nas investigações criminais, como acima já mencionado, são: o ***man-in-the-midle*** e o ***hacking***. Na prática, operar-se-ia da seguinte forma[62]:

> Há duas saídas que permitiriam que o WhatsApp encaminhasse o conteúdo de futuras mensagens para o Estado. [...] Essas duas saídas, entretanto, exigiriam ou que a empresa se dispusesse a atuar como intermediário no repasse das mensagens para o Estado, burlando seu próprio sistema de criptografia, ou modifique o funcionamento técnico do aplicativo. A primeira saída é uma técnica conhecida como ataque do tipo '**man-in-the-middle**'. Para a criptografia entre duas partes funcionar, elas devem trocar suas chaves públicas (public keys). O WhatsApp faz essa troca de chaves para você. Nesse processo, o aplicativo poderia decidir dar para as partes a chave privada e pessoal do WhatsApp em vez da que seria a correta. A partir daí, o WhatsApp conseguiria receber todas as mensagens que as duas partes enviassem uma para a outra, recriptografá-las com a chave correta e fingir que nada aconteceu. [...] No WhatsApp, esse procedimento pode ser feito ao escanear o código de segurança um do outro. A segunda saída é uma técnica que exigiria modificar o aplicativo para que ele mandasse (algumas) **mensagens para o Estado** além de enviá-las para o destinatário original. O WhatsApp poderia implementar esse 'recurso' da mesma forma que fez com a criptografia de ponta a ponta: publicando uma versão nova do aplicativo nas lojas de aplicativos (AppStore e outras). Essa seria a única alternativa técnica para o WhatsApp conseguir armazenar o conteúdo das mensagens. Mesmo assim, um usuário habilidoso ainda conseguiria descobrir se o seu aplicativo estiver encaminhando suas mensagens para o Estado.

Interessante notar que os meios e soluções para uma tentativa de consenso, ainda que de forma parcial, são lotados de meios-termos, porém, acabam não destoando radicalmente, porque todas destacam a defesa de direitos e garantias fundamentais ínsitas de países dotados de um estado democrático e voltam-se a uma mesma tecnologia (E2EE).

Conclui-se, portanto, que os pontos nodais de divergência são em virtude dos alicerces históricos e sociais de cada Nação. Modelo disso são os Estados Unidos, que prezam muito à liberdade de expressão, porém, de igual maneira, como potência econômica e militar[63], participam de inúmeras guerras e são alvo de ataques

---

[62] *Ibid.*

[63] AHLAM, Rafita. Apple, the Government, and You: Security and Privacy Implications of the Global Encryption Debate. **Fordham International Law Journal**, v. 44, n. 3, 2021. Disponível em: https://ir.lawnet.fordham.edu/ilj/vol44/iss3/5. Acesso em: 26 nov. 2021: as políticas dos EUA "terão um **impacto internacional**. [A] **criptografia é em grande parte um problema de engenharia que requer cooperação entre empresas de tecnologia e governos**" (p. 845-846; tradução e grifo nossos).

terroristas, o que demanda uma força investigativa (preventiva) de elevadíssima relevância em nome da segurança nacional[64], sob a premissa legal e jurisprudencial das chamadas "circunstâncias exigentes". A apreensão policial imediata em computadores nessas circunstâncias, sob pena de se apagarem os dados, é aceita no direito norte-americano (há ressalvas, como será visto no caso Riley v. Califórnia, subcapítulo 3.1.3 deste trabalho):

> Os dados do computador podem ser efetivamente colocados fora do alcance da aplicação da lei com programas de **criptografia** amplamente disponíveis e poderosos que podem ser acionados com apenas poucos toques de tecla. Além disso, comandos de computador podem destruir dados em uma questão de segundos, assim como umidade, alta temperatura, mutilação física ou campos criados, por exemplo, passando um forte ímã sobre um disco. Por exemplo, nos Estados Unidos v. David, 756 F. Supp. 1385 (D. Nev. 1991), os agentes viram o réu apagando arquivos em seu computador e apreendeu o computador imediatamente. O tribunal distrital considerou que **os agentes não precisavam de um mandado para apreender o computador porque os atos do réu criaram circunstâncias exigentes**.[65] (Tradução e grifo nossos).

Talvez em outras Nações, a segurança pública, ou a garantia de uma justiça penal mais ativista seja o valor que prepondere, gerando o dissenso. Na Alemanha, por exemplo, busca-se um equilíbrio entre os direitos dos cidadãos e o dever de garantir que o crime não permaneça impune, o que nem sempre é consenso em novas legislações, demandando ações constitucionais[66].

É necessário novamente alertar para uma especial diferença na discussão sobre a eliminação da criptografia ponta a ponta, ou a criação de chaves para acesso em investigações criminais: apesar de contenda em casos concretos sobre a possibilidade de determinação judicial a empresas de tecnologia para uma interceptação telemática por crime grave, sua defesa, em muitos países, dá-se, por ora, apenas antes disso, no plano abstrato (como o acadêmico, político e da mídia).

Ora, ao se raciocinar ainda no plano em abstrato, fora de um caso em concreto, de qual direito ou garantia deva prevalecer, a ponderação de princípios

---

[64] A respeito, registre-se roteiro histórico-normativo sobre a interceptação telefônica em atos de segurança nacional: UNITED STATES GOVERNMENT. Bureau of Justice Assistance. **The Foreign Intelligence Surveillance Act of 1978 (FISA)**. Disponível em: https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1286. Acesso em: 12 dez. 2021.

[65] JARRETT, H. Marshall; BAILIE, Michael W. **Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.** 3. ed. Office of Legal Education - Executive Office for United States Attorneys. Disponível em: https://www.justice.gov/file/442111/download. Acesso em: 19 set. 2022, p. 28.

[66] Como será visto no subcapítulo 3.3.

constitucionais fica prejudicada, até porque vai de encontro à correta técnica preconizada por Robert Alexy, a exemplo do argumento da defesa da segurança nacional (ou de circunstâncias exigentes). Veja-se[67]:

> Se dois princípios colidem — o que ocorre, por exemplo, quando algo é proibido de acordo com um princípio e, de acordo com o outro, permitido —, um dos princípios terá que ceder. Isso não significa, contudo, nem que o princípio cedente deva ser declarado inválido, nem que nele deverá ser introduzida uma cláusula de exceção. Na verdade, o que ocorre é que um dos princípios tem precedência em face do outro **sob determinadas condições.** Sob outras condições a questão da precedência pode ser resolvida de forma oposta. Isso é o que se quer dizer quando se afirma que, **nos casos concretos, os princípios têm pesos diferentes e que os princípios com o maior peso têm precedência.** Conflitos entre regras ocorrem na dimensão da validade, enquanto as colisões entre princípios — visto que só princípios válidos podem colidir — ocorrem, para além dessa dimensão, na dimensão do peso.

Destarte, abstratamente, o raciocínio pode ser defendido em favor de ambos os posicionamentos, especialmente por proteger os cidadãos da livre manifestação em países antidemocráticos, de um lado, e, do outro, evitar atos de guerra, ou terroristas, ao permitir um maior controle do Estado de conversas em investigações criminais dotadas de E2EE. E, no Brasil, o caso concreto já restou fixado no Supremo Tribunal Federal (ADPF 403 e ADI 5527), apesar de ainda sob julgamento do mérito.

Não por acaso e de forma correta, portanto, extrai-se de parte do voto do Min. Relator Edson Fachin (ADPF 403) expressa aplicação da teoria de Robert Alexy. Motiva-se no voto o necessário estudo de premissas técnicas ("certeza científica") da área da informática trazidas pelas partes e interessados envolvidos nos autos. A questão-chave para enfrentar o mérito é

> [...] **saber se o risco público representado pelo uso da criptografia justifica a restrição desse direito por meio da imposição de soluções de software, como, por exemplo, a proibição da criptografia ou a criação de canais excepcionais de acesso ou pela diminuição do nível de proteção.** A resposta a essa questão depende de um rigoroso exame de **proporcionalidade**, isto é, de uma avaliação cuidadosa para se o que se ganha com a promoção de um interesse público é ou não compensado com a restrição de direitos. Além disso, **é preciso que a Corte leve em devida conta a certeza científica que se tem sobre essas informações**, assim como o grau de institucionalização promovido pelo Estado. Afinal, **"quanto mais grave for o peso de uma interferência em um direito constitucional,**

---

[67] ALEXY, Robert. **Teoria dos direitos fundamentais.** Tradução: Virgílio Afonso da Silva. São Paulo: Malheiros, 2008, p. 93-94. Adicione-se ao defendido pela moderna doutrina alemã, de um modelo de "proceduralização" do direito, conforme rodapé n. 323.

> **maior deve ser a certeza sobre as premissas que a fundamentam**" (ALEXY, Robert. On Balancing and Subsumption. A Structural Comparison. **Ratio Juris**, v. 16, n. 4, dez. 2003, p. 446). "O voto estrutura-se, portanto, no exame dos argumentos sobre os direitos envolvidos e sobre a intensidade da interferência neles causada a partir de possíveis alterações no modelo de criptografia adotado pelo Whatsapp". [68] (Grifo nosso).

Além disso, em caso de decisão pela quebra da criptografia, ainda que pela Suprema Corte de país fora da sede (caso do Brasil em face do WhatsApp), haveria possível desobediência de cumprimento[69], como já ocorreu em casos semelhantes[70], ou, talvez o próprio cancelamento dos serviços no Brasil por iniciativa da empresa; exceto, claro, por uma facilidade decorrente de eventual concretização de reforma legislativa e jurisprudencial nos EUA no mesmo sentido de futura decisão no STF quanto à E2EE. E, parece ser esta uma das dificuldades em se estabelecer um critério objetivo e uníssono da melhor solução possível para essa celeuma.

Sobre a responsabilidade de as *Big Techs* cumprirem decisões judiciais há recente entendimento judicial envolvendo o Google[71], determinando-se o cumprimento dos mandados judiciais mesmo estas empresas optando armazenar os dados eletrônicos contidos no mandado em seus próprios servidores no exterior, no sentido de serem infundadas as recusas nos casos de crimes praticados dentro dos EUA, por pessoas que se comunicavam por *e-mail* neste país, em realizar a guarda de tais e-mails em outros países. Porém, há julgamento, por maioria, em face da Microsoft, em sentido contrário, ou seja, exigindo-se que os dados armazenados também estejam dentro do território norte-americano[72] (no caso, a Microsoft foi desobrigada de produzir ao governo o conteúdo da conta de e-mail de um cliente armazenado na Irlanda), demandando divergência crítica do juízo (REENA RAGGI,

---

[68] BRASIL. Supremo Tribunal Federal. **ADPF 403/SE**. *Op. cit*, p. 55.

[69] Vide o rodapé n. 353 sobre o julgamento do ADC 51 e suas implicações na cooperação jurídica internacional em matéria probatória penal.

[70] Em casos como LICRA v. *Yahoo* e Alemanha v. Töben, fica evidente ser "comum que decisões judiciais de uma nação não recebam *exequatur* nos territórios em que deveriam ser cumpridas, o que ocorre por diversos motivos, inclusive de natureza política" (Cf.: LEONARDI, Marcel. **Fundamentos de direito digital**. São Paulo: Thomson Reuters Brasil, 2019, p. 140-147).

[71] BLANCO, Kenneth. An important Court opinion holds lawful warrants can be used to obtain evidence from U.S. internet service providers when those providers store evidence outside the U.S. U. S. **Department of Justice**, Washington, DC, 6 Feb. 2017. Disponível em: https://www.justice.gov/archives/opa/blog/important-court-opinion-holds-lawful-warrants-can-be-used-obtain-evidence-us-internet. Acesso em: 20 set. 2022.

[72] UNITED STATES. Microsoft Corporation v. United States of America. Decisão de 14 jul. 2016. Disponível em: https://www.justice.gov/archives/opa/blog-entry/file/937006/download. Acesso em: 20 set. 2022. Em síntese: "Concluímos que o Congresso não pretendia que as disposições do mandado da SCA [Stored Communications Act...] se aplicassem extraterritorialmente" (p. 13; tradução nossa).

Circuit Judge) no sentido de se neutralizar qualquer responsabilidade dos provedores em casos relevantes de segurança nacional no combate a crimes graves, referindo-se a aludida magistrada ao atentado terrorista do *World Trade Center*[73], dado o absurdo desproporcional de princípios e que o cumprimento do mandado judicial se daria por pessoa dentro do território dos EUA.

A divergência nos posicionamentos quanto à E2EE iniciou-se da falta de interesse comercial e ideológico das empresas que se utilizam dessa tecnologia da criptografia almejarem tomar outra postura que não seja mantê-la, sem exceções, alegando, simplesmente, impossibilidade técnica, mas sempre, frisando a defesa de preceitos constitucionais que legitimam seu lado da história, o que é verdade, apesar do interesse empresarial (econômico), talvez aqui de forma mais velada[74], ou, inadmitida publicamente (só por descuido)[75].

O cerne da questão é encontrar alguma solução tecnológica para o problema, uma tendência que já se verifica quanto à relevância dos pareceres técnicos para resolução de diversos conflitos judiciais nos quais não se traz clareza para uma decisão judicial que dependa das normas simplesmente, da equidade ou das máximas da experiência do magistrado, principalmente nas questões científicas, incluindo a tecnologia.

Apesar da cientificidade desse ramo, as opiniões se dividem, e isso repercute na decisão judicial de forma prejudicial a uma melhor análise dos fatos. Os argumentos ideológicos acabam prevalecendo por todos os setores pesquisados (Poderes Executivo e Legislativo, polícia, Ministério Público, doutrinadores e especialistas em tecnologia)[76]. Talvez por estarmos num processo de construção de uma sociedade ligada por novas tecnologias revolucionárias, digitalmente conectada

---

[73] Pelo raciocínio do julgado "se o governo conseguisse demonstrar causa provável para acreditar que [terroristas do 11 de setembro] estivessem se comunicando eletronicamente sobre um ataque iminente e devastador [...] e que a Microsoft possuía esses e-mails, nenhum tribunal federal poderia ter emitido um mandado", obrigando-a a recuperar esses e-mails caso armazenados no exterior, **mesmo que sediada e executável a medida nos EUA** (*Ibid.*, p. 2; tradução e grifo nossos).

[74] Como o pagamento através do aplicativo. In: OLIVEIRA, João José. WhatsApp libera transferência de dinheiro no Brasil pelo serviço, mas ainda não para todo mundo. **UOL**, São Paulo, 4 maio 2021. Disponível m: https://economia.uol.com.br/noticias/redacao/2021/05/04/whatsapp-vai-permitir-envio-de-dinheiro-para-pessoas-a-partir-de-hoje.htm. Acesso em: 12 dez. 2021.

[75] Conforme constatado no rodapé n. 41.

[76] À organização da convivência da humanidade de forma democrática, defende-se a necessidade de um imperativo jurídico e político universais, com vistas à legitimação desta coação não exclusivamente ao interesse do Estado, mas também, voltada aos interesses dos cidadãos afetados. Cf.: HÖFFE, Otfried. **Derecho intercultural**. Tradução: Rafael Sevilla. Barcelona: Gedisa, 2008, p. 229 e 246).

e a caminho de um sistema jurídico globalizado seja salutar à construção desse debate[77], mas há aspectos negativos nisso, como a imposição de regras pelo Estado para solucionar a questão por inércia e acumulação de poder nas mãos de poucas empresas, que afetam valores relevantíssimos ao estado democrático e constitucional de direito. Por isso a doutrina[78] vem preconizando que

> [...] a comunicação produzida pelo STF (e por qualquer outro tribunal) pode tanto gerar novo valor informativo dentro do sistema jurídico, como **também pode circular para além dele.** Portanto, o papel desempenhado pelo tribunal deve ser compreendido à luz da complexidade dos processos da sociedade mundial e a partir de uma constelação de outros tribunais que o circunda. (Grifo nosso).

Cansados desse panorama, os países estão criando alternativas práticas e soluções legislativas; a pressão sobre as *Big Techs* é enorme e já repercutem na limitação da criptografia ponta a ponta a novas ferramentas no Facebook e Instagram, além de recentes declarações de meios de melhora de segurança digital do ponto de vista da proteção às crianças e adolescentes. Logo, imperativo breve exame desses países na implementação de suas atuações.

Destaque-se o pronunciamento no *site* oficial do governo do Reino Unido[79], em manifesto intitulado "*International statement: End-to-end encryption and public safety (accessible version)*", de 11 de outubro de 2020, assinado por representantes deste país e dos Estados Unidos, Austrália, Nova Zelândia, Índia e Japão, no sentido da importância da criptografia ponta a ponta à privacidade e outros valores democráticos, contudo, também, da segurança pública e do dever das empresas empreenderem esforços para ultrapassar toda essa celeuma:

> Em julho de 2019, os governos do Reino Unido, Estados Unidos, Austrália, Nova Zelândia e Canadá emitiram um comunicado, concluindo que: "as

---

[77] Ora, "**o direito é um fenômeno mutável nas suas fronteiras, plural nas suas fontes de criação e revelação**, complexo na sua lógica interna, não consistente nem harmônico nos seus conteúdos, e, finalmente, nada afeito a um saber que retenha certezas e formulações seguras e não opináveis. [...] **sujeito** [...] **ao convívio e à disputa de outras ordens normativas**" (HESPANHA, Antônio Manuel. **Pluralismo jurídico e direito democrático**. São Paulo: Annablume, 2013, p. 19).

[78] BARROS, Marco Antonio Loschiavo Leme de. **Tribunais, complexidade e decisão**: o argumento consequencialista no direito brasileiro. 2018. 95 f. Tese (Doutorado em Direito) – Universidade de São Paulo, 2018. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2139/tde-30102020-152804/publico/6476260_Tese_Parcial.pdf. Acesso em: 18 ago. 2021, p. 333.

[79] UNITED KINGDOM. International statement: End-to-end encryption and public safety. **Gov.UK**, Oct. 11 Oct. 2020. Disponível em: https://www.gov.uk/government/publications/international-statement-end-to-end-encryption-and-public-safety/international-statement-end-to-end-encryption-and-public-safety-accessible-version. Acesso em: 15 nov. 2021.

> **empresas de tecnologia devem** incluir mecanismos no design de seus produtos e serviços **criptografados** por meio dos quais os governos, **agindo com autoridade legal apropriada, pode obter acesso aos dados em um formato legível e utilizável**. Essas **empresas** também **devem** incorporar a segurança de seus usuários em seus projetos de sistema, permitindo-lhes tomar medidas contra o conteúdo ilegal".
> Em 8 de outubro de 2019, **o Conselho da UE** adotou suas conclusões sobre o combate ao abuso sexual infantil, declarando: "O Conselho **insta a indústria** a garantir o acesso legal das autoridades policiais e de outras autoridades competentes às provas digitais, inclusive quando **criptografadas** ou hospedadas em servidores de TI localizado no exterior, **sem proibir ou enfraquecer a criptografia e em total respeito às garantias de privacidade e julgamento justo** consistentes com a lei aplicável. " [...].
> Estamos comprometidos em trabalhar com a indústria para desenvolver **propostas razoáveis que permitirão que empresas de tecnologia e governos protejam o público e sua privacidade, defendam a segurança cibernética e os direitos humanos e apoiem a inovação tecnológica.** Embora esta declaração se concentre nos desafios apresentados pela **criptografia de ponta a ponta**, esse compromisso se aplica a toda a gama de serviços criptografados disponíveis, incluindo criptografia de dispositivo, aplicativos criptografados personalizados e criptografia em plataformas integradas.
> Reiteramos que a proteção de dados, o respeito pela privacidade e a importância da criptografia à medida que a tecnologia muda e os padrões globais da Internet são desenvolvidos permanecem na vanguarda da estrutura legal de cada estado. No entanto, **desafiamos a afirmação de que a segurança pública não pode ser protegida sem comprometer a privacidade ou a segurança cibernética.** Acreditamos **fortemente** que as abordagens que protegem cada um desses valores importantes são possíveis e **nos esforçamos para trabalhar com a indústria para colaborar em soluções mutuamente aceitáveis**. (Tradução e grifo nossos).

As cartas foram postas na mesa por essas potentes Nações; e as *Big Techs* já deram notícias de uma adaptação, no mínimo, de um recuo em adicionar a criptografia ponta a ponta a outros aplicativos. De qualquer forma, o Legislativo e o Judiciário, independentemente desses atos de governo, já estão demandando das empresas há certo tempo, como adiante analisado, ensejando discussões sobre a responsabilidade penal, civil e administrativa das pessoas jurídicas.

2.4 AS RESPONSABILIDADES DAS PESSOAS JURÍDICAS NA PRODUÇÃO DA PROVA PENAL DIGITAL COMO UMA CONTRIBUIÇÃO À SUA EFETIVIDADE E APLICAÇÃO NO BRASIL

De todo o problema preambular plantado, é pacífico que a comunicação digital dotada da tecnologia da E2EE evidencia crise inexistente até pouco tempo nas investigações criminais, quando aberta a possibilidade constitucional, nos países democráticos e sob o crivo do devido processo legal, da intervenção estatal na esfera

da privacidade dos investigados, com cooperação das empresas privadas à efetivação da interceptação telefônica e telemática.

Até poucos anos atrás, quando inexistente o serviço de mensageria digital dotada de criptografia ponta a ponta, basicamente só a telefônica, as questões dogmáticas divergentes eram, em suma, as restritas a requisitos e interpretações legais, como: a) a possibilidade da interceptação telefônica para apuração de delito punido com detenção, caso conexo com um de reclusão[80]; b) o disposto na Tese 661 do STF: a licitude das sucessivas renovações de interceptação telefônica, desde que motivada no caso concreto a necessidade da medida complexa e preenchidos os requisitos da lei[81]). Mas, sempre foi possível a interceptação telefônica pela tecnologia propiciar tal ato, dentro dos limites legais e constitucionais. Agora, a E2EE trouxe esta necessidade: o auxílio material (tecnologia possível) do setor privado, hoje inexistente, sem a qual a prova penal digital, mesmo deferida por ato judicial, torna-se impossível pelos meios disponíveis pela ciência.

Por tal motivo, a resistência da E2EE foi evidenciada nos capítulos anteriores, mas revela, em síntese, a preparação de uma resposta pelo Estado, dentro das peculiaridades de cada país e de algumas intervenções conjuntas para, além do incurso do Poder Judiciário e Legislativo, advir a intervenção política estatal, ainda que num viés colaborativo com as chamadas *Big Techs*, associado à pressão inerente das grandes Nações.

O relevante a ser dito, como pano de fundo às legítimas pretensões e conflito de princípios constitucionais, é que está sendo preparado o papel de garante dessas pessoas jurídicas de direito privado, por determinação legal[82], evitando-se escapes na desobediência de decisões judiciais na seara investigativa criminal quanto a pedidos de interceptação telemática deferidos. Cabe um alerta, todavia. É que a doutrina (e no presente ponto será usada como base a teoria da ação significativa) elenca como

---

[80] BRASIL. Superior Tribunal de Justiça. Interceptação Telefônica – I. **Jurisprudência em Teses**, Brasília, n. 117, 25 jan. 2019. Disponível em: https://scon.stj.jus.br/SCON/jt/toc.jsp. Acesso em: 9 jul. 2022.

[81] BRASIL. Supremo Tribunal Federal. Tema 661 – STF: Possibilidade de prorrogações sucessivas do prazo de autorização judicial para interceptação telefônica. **Diário da Justiça Eletrônico**, 6 jun. 2022.

[82] As sanções em pecúnia às *Big Techs* têm se revelado ineficazes, demonstrando que a "sociedade necessita urgentemente de um sistema claro de responsabilidade legal" (MENEZES, Cyntia S. de; AGUSTINA, José R. Big data, inteligencia artificial y policía predictiva: bases para una adecuada regulación legal que respete los derechos fundamentales. In: KIEFER, Mariana (Coord.). **Cibercrimen III**. Buenos Aires: BdeF, 2020). (p. 179, tradução nossa).

limite interpretativo na análise da função de garante ao significado subsumido ao caso concreto ante um conceito legal aberto:

> [...] a possibilidade da comissão por omissão deriva do significado de uma conduta. **Não pode, pois, haver um conceito geral. Será em cada caso** a partir dos verbos típicos e do contexto valorativo específico que haverá que decidir se o substrato da conduta omissiva em juízo resulta subsumível à formulação legal do delito.[83] (Tradução e grifo nossos).

Na Espanha, desde a Lei n. 34/2002 (Lei de Serviços da Sociedade da Informação e do Comércio Eletrônico – LSSI)[84] preconiza-se, apesar de não tratar especificamente da E2EE, a incumbência censora que se deve evitar às empresas privadas (as provedoras dos serviços de *internet*), dado o receio de uma função de garante universal (dever de cuidado[85]) e a consequente responsabilidade (penal, civil, ou administrativa) objetiva da pessoa jurídica, ponto nodal limitativo correto, a se impor noutras legislações.[86]

Do posicionamento doutrinário, defende-se também que o artigo 16 dessa lei espanhola promove o afastamento de uma função de controle pelas empresas privadas do que seja ou não lícito, ou "a verdade", questão fática que vem se percebendo por todo o mundo[87]:

> O que esse preceito busca evitar é que os provedores – diante da **ameaça de poderem ser considerados responsáveis ou inclusive sancionados penalmente** por haverem contribuído com a manutenção dos seus serviços para a publicação ou divulgação de conteúdos alheios – possam optar por impedir a publicação ou divulgação de qualquer conteúdo ou informação que tenha a mínima aparência de ser ilícita; **opção que, ainda que muito provavelmente, lhes levaria a impedir a publicação de muitas informações penalmente ilícitas ou nocivas, também lhes levaria, certamente, a impossibilitar a divulgação de muitas outras**

---

[83] Cf.: CUERDA ARNAU, María Luisa. Limites constitucionales de la comisión por omisión. **Justiça e Sistema Criminal**, Curitiba, v. 6, n. 10, jan./jun. 2014, p. 106. Disponível em: https://revistajusticaesistemacriminal.fae.edu/direito/article/view/15/13. Acesso em: 4 jul. 2022.

[84] **"Art. 16. Responsabilidade dos provedores** de serviços de hospedagem ou armazenamento de dados. 1. [...] não serão responsáveis pela informação armazenada [...] desde que: **a) Não tenham conhecimento efetivo** de que a atividade ou informação armazenados seja ilegal [ou] **b) Se os tiver, aja com diligência para remover**" (Tradução e grifo nossos). ESPAÑA. Ley 34/2002. **BOE**, n. 166, 12 jul. 2002. Disponível em: https://www.boe.es/eli/es/l/2002/07/11/34/con. Acesso em: 21 out. 2022.

[85] Conforme enfatiza o projeto de lei do Reino Unido, conforme subcapítulo 3.2.

[86] Vide: GALÁN MUÑOZ, Alfonso. A responsabilidade penal dos provedores de serviço na internet pela divulgação de conteúdos ilícitos: uma reflexão inicial sobre o regime espanhol e o brasileiro. **Justiça e Sistema Criminal**, Curitiba, v. 6, n. 11, jul./dez. 2014. Disponível em: https://revistajusticaesistemacriminal.fae.edu/direito/article/view/30. Acesso em: 3 jul. 2022. (p. 94).

[87] Como o fato público e notório de reiteradas alegações de indevida censura prévia, com o consequente bloqueio de vídeos e postagens das redes sociais de diversos usuários pelas próprias mantenedoras desses serviços digitais na rede digital, mesmo sem decisão judicial a respeito.

> **perfeitamente lícitas e permitidas, transformando-se a rede, assim, num meio de comunicação censurado e amordaçado**; um ambiente no qual os cidadãos não poderiam exercer de uma forma plena seus direitos à liberdade de expressão e de informação.[88]

E, de uma forma ou de outra, quanto ao momento que passa a ser responsável por atos de terceiros, segundo a legislação espanhola, advém o receio (tal como nos projetos de lei dos EUA e do Reino Unido, subcapítulos 3.1.5.2 e 3.2, respectivamente) de os provedores acabarem sendo forçados a quebrar a E2EE para o cumprimento da determinação judicial, conforme:

> Noutras palavras, o que faz o art. 16.1 "b" LSSI não é criar um novo dever de atuar do provedor que o obriga a apagar ou bloquear o conteúdo em questão e que no caso de ser descumprido torne-o responsável pela divulgação **(o dever de garante)**, mas **definir o modo pelo qual haveria de cumprir com dito dever ("com diligência"), quando o tenha, para poder continuar isento de responsabilidade pela prestação de seus serviços.** Com isso, o que essa prescrição faz é **converter o dever objetivo de cuidado** dos intermediários que conheçam a ordem de retirada ou a declaração de ilicitude do conteúdo que armazenam, referindo-se que **esses sujeitos terão que respeitar o momento de cumprir com o dever de retirada, civil, penal ou administrativo que lhes pudesse corresponder, para continuarem isentos de responsabilidade jurídico pela prestação de seus serviços, o que evidentemente, permitirá que lhes seja imputada responsabilidade por não haverem cumprido adequadamente com esse dever,** [...]**. Se eliminará assim toda possibilidade de existir qualquer tipo de responsabilidade objetiva desses provedores pelas ações ou omissões que tenham podido efetuar**, o que, ainda que no Direito penal esteja fora de qualquer dúvida como consequência da estrita exigência do princípio da culpabilidade, em outros âmbitos, como o civil, poderia chegar a questionar-se.[89]

No Brasil, temos vivenciado esse assunto não só pelas referidas ações constitucionais específicas quanto à figura na mensageria digital ponta a ponta relevantes ao direito penal e processual penal, mas fatos correlatos em várias outras normativas, como, recentemente, no processo eleitoral, do qual se extrai a relevância da participação efetiva das grandes empresas de mídia digital.

O Presidente do TSE (2022), Min. Alexandre de Moraes, chegou a se reunir com representantes de plataformas digitais e redes sociais – tal como o Google, Meta (Facebook, Instagram, WhatsApp), Twitter, TikTok, Likedin, Twitch, Kwai e Linkedin, ausente do Telegram –, para solicitar vigilância no combate à propagação de

---

[88] *Ibid.*, p. 90.
[89] *Ibid.*, p. 94.

desinformação e notícias falsas na campanha eleitoral antes do segundo turno[90], reforçando um regime de responsabilização e cooperação entre o Estado e os particulares. Ilustre-se, como exemplo, as incisivas intervenções normativas do TSE no seu exercício do poder de polícia, quanto a eventuais crimes contra o Estado Democrático de Direito, em serviços de mensageria privada nas eleições presidenciais do Brasil de 2022.[91]

No tema específico quanto à responsabilidade penal da pessoa jurídica, vale ressaltar que na toada da globalização de um sistema de produção de provas penais digitais efetivo, a Convenção de Budapeste[92] (art. 20, no caso de interceptação telemática em tempo real) é só uma demonstração da escala que essa pretensão de diversos países está tomando, sem falar de atitudes de viés político de vários Estados[93]. Ocorre que, aliado ao papel de garante, deve vir, sob pena de uma função isenta de obrigação da pessoa jurídica, o meio material para a consecução da quebra da criptografia, por tecnologia tida como inexistente, ou, a retirada de tal tecnologia, gerando a polêmica da ofensa a outros princípios resguardados após o advento da E2EE.

Sobre o complexo tema da delimitação da figura do "garantidor", há posicionamento doutrinário para motivar o cabimento da responsabilidade penal dos provedores de *internet* nos casos da E2EE em mensagens que se almeja a interceptação telemática[94]:

> A ideia fundamental é a de filtrar os critérios fixados pela **lei** através de dois outros critérios fundamentais, quais sejam, **a guarda de um bem jurídico concreto** (criadora de deveres de *proteção* e *assistência*) e o **domínio material sobre uma fonte de perigo** (determinante de deveres de segurança e controle).

---

[90] In: BRASIL. Tribunal Superior Eleitoral. **TSE e plataformas digitais discutem reforço contra desinformação no 2º turno**. Brasília, 19 out. 2022. Disponível em: https://www.tse.jus.br/comunicacao/noticias/2022/Outubro/tse-e-plataformas-digitais-discutem-reforco-contra-desinformacao-no-2o-turno-1. Acesso em: 25 nov. 2022.

[91] A respeito: BRASIL. Supremo Tribunal Federal. Medida Cautelar em ADI n. 7.261/DF. Relator: Min. Edson Fachin. Brasília, DF, 22 out. 2022. Disponível em: https://www.conjur.com.br/dl/adi7261-indeferid.pdf. Acesso em: 25 nov. 2022.

[92] Como será esmiuçado no subcapítulo 4.3; mas, como dito, é o tratado internacional, aderido pelo Brasil, para sistematizar o tema "crimes cibernéticos e o direito processual penal", por cooperação probatória internacional, como a interceptação telemática (BRASIL. Câmara dos Deputados. **MSC 412/2020**. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2258985. Acesso em: 18 nov. 2021).

[93] Demonstrado no rodapé n. 79.

[94] In: BUSATO, Paulo César. **Direito penal**: parte geral. 6. ed. São Paulo: Tirant lo Blanch, 2022, p. 223.

E, neste caso, a obrigação jurídica deriva de um "poder de disposição" capaz de gerar "situações perigosas" a terceiros, e, o resultado "**será imputável** se, também segundo uma consideração *ex post*, se comprovar que aquela diminuição [do risco possível] se teria efetivamente verificado".[95]

Como já aduzido, encaminha-se, enquanto não se resolve esta questão tecnológica da E2EE, para um sistema jurídico único[96], ou mais perto disso possível, não só pela coerência fática, mas também a jurídica, do problema posto no caso desses aplicativos de mensageria digital utilizados por bilhões de pessoas por todo o mundo. Por tal razão, defende-se[97] a necessidade de se criar uma metodologia de julgamento diferenciada em casos como o da E2EE:

> [...] a crescente internalização por tratados e convenções internacionais em nosso ordenamento jurídico, e, casos difíceis idênticos quanto à matéria fática-problema, mesmo sem o imperativo legal ou supralegal de obediência, como ocorre em decisões da Corte Internacional de Direitos Humanos, devem, seguindo os critérios da universalidade e da coerência normativa do doutrinador ora em estudo, ser utilizados como critérios interpretativos pelos magistrados da Suprema Corte nos julgamentos, como se fosse uma matéria preliminar de seus votos, ou, mesmo inerente à motivação do mérito da decisão. O autor [Neil MacCormick] não tratou deste tema específico em seus estudos, mas seus métodos interpretativos norteiam esta possível aplicação, em destaque na sociedade globalizada pela tecnologia, principalmente. Com isso, evita-se decisão discrepante em casos idênticos no âmbito internacional, trazendo segurança jurídica aos cidadãos em escala mundial, com repercussão nas esferas pública (direito penal e processual penal) e privada (direito à privacidade e à liberdade de informação), o que aprimora ainda mais o Estado Democrático de Direito.

Aliás, "O ordenamento jurídico em vigor no Brasil não admite a defesa de uma vinculação das cortes nacionais à jurisprudência internacional, entretanto esta deve ser observada e valorada, ainda que não seja seguida"[98], tal como se verifica da norma

---

[95] *Ibid.*, p. 224.

[96] Observa-se que "o direito moderno mantém elevada interdependência com os demais sistemas (p. ex., econômico, político, científico etc.). [...] o **sistema jurídico é um só**. [...] A globalização demanda novas diferenciações no interior do sistema jurídico, mas não é capaz de corromper sua função (Grifo nosso. CAMPILONGO, Celso Fernandes. **O direito na sociedade complexa**. 2. ed. São Paulo: Saraiva, 2013, posição 1879).

[97] COSTA, Daniel Tempski Ferreira da; ROSA, Luísa Walter da. A resolução de casos difíceis a partir do pensamento de Neil MacCormick: a necessidade da análise de precedentes das Supremas Cortes de nações democráticas. **Interfaces Científicas**: Direito, Aracaju, v. 9, n. 1, p. 110-123, 2022. DOI: 10.17564/2316-381X.2022v9n1p110-123. Acesso em: 30 jun. 2022.

[98] OLIVEIRA, Larisse Silva. **Diálogos jurisdicionais entre o STF e a Corte Interamericana: comunicações transjudiciais e jurisprudência internacional de direitos humanos**. Belo Horizonte; São Paulo: D'Plácido, 2020, p. 122.

interpretativa do art. 29, b[99], da CADH, sabendo-se de obstáculos a um diálogo jurisdicional à utilização de jurisprudência estrangeira nas motivações judiciais, inclusive no direito norte-americano, este, em "posição refratária [...] no caso das interações transjudiciais[100]". Extrai-se do dispositivo supracitado, a aplicação do princípio *pro homine*, inexistindo supremacia de regramento internacional sobre o ordenamento jurídico interno.

Porém, nada impede o intuito de se estabelecer um mote isento de pré-conceitos, em linha a fundamentos não últimos ou únicos, no uso de aprimoramento dos entendimentos (ensinamentos) de outras Nações, pois a

> utilização das teorias dialógicas, contrárias às teorias da última palavra definitiva e às teorias supremacistas, permite uma abertura a processos deliberativos de decisão que considerem diferentes perspectivas, admitindo uma interpretação que decorra dos fundamentos utilizados e não baseada apenas na autoridade que a realizou[101].

E a cooperação jurídica internacional quanto à produção da prova penal digital, tal como na Convenção de Budapeste, demonstra uma convivência de tradições jurídicas distintas, corroborada tal possibilidade integrativa pela doutrina[102]:

> O estudo das bases filosóficas que remontam a Wittgenstein inspiraram autores, tanto no plano do direito continental quanto do *common law*, no que se refere à reforma da estrutura do sistema de imputação, a partir de tais fundamentos epistemológicos, em especial no que refere ao conceito de ação **[emergindo], em ambos os cenários jurídicos, concepções que guardam estreita proximidade.**

Pelo conjunto desse modo de raciocínio, a posição do setor privado de simplesmente criar uma tecnologia que torne a produção da prova impossível ao legítimo interesse estatal de interceptação telemática por países democráticos não iria ficar sem qualquer reação. A questão da E2EE gera um meio quase livre de punição, com exceção dos já indicados meios alternativos de produção de prova. Mas, para

---

[99] "Nenhuma disposição desta Convenção pode ser interpretada no sentido de: [...] b) limitar o gozo e exercício de qualquer direito ou liberdade que possam ser reconhecidos de acordo com as leis de qualquer dos Estados-Partes ou de acordo com outra convenção em que seja parte um dos referidos Estados" – BRASIL. Decreto n. 678, de 6 de novembro de 1992. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/d0678.htm. Acesso em 12 set. 2022.

[100] OLIVEIRA, Larisse Silva. *Op. cit*, p. 101.

[101] LEAL, Mônia Clarissa Hennig; MORAES, Maria Valentina de. **Margem de apreciação nacional e diálogo institucional e entre cortes na perspectiva do Supremo Tribunal Federal e da Corte Interamericana de Direitos Humanos**. São Paulo: Tirant lo Blanch, 2021, p. 194.

[102] BUSATO, Paulo César. Delitos de posse e ação significativa – crítica aos Besitzdelikte a partir da Concepção Significativa da Ação. **Sequência**, Florianópolis, n. 73, maio/ago. 2016; p. 91; grifo nosso.

além disso, retira totalmente a posição de garante das pessoas jurídicas responsáveis pela tecnologia em suas plataformas digitais (como o WhatsApp e o Telegram), ainda que por lei prevista tal responsabilização e dada situação concreta.

A filosofia da linguagem funciona como uma base científica universal, auxiliando na integração entre os diversos ordenamentos jurídicos em seus fundamentos, e é concretizada na concepção significativa da ação como modo de pensar no caso da E2EE. Logo, como tecnologia inovadora por todo o mundo a qual, em regra, é obstativa do conhecimento desta ação comunicativa pelas autoridades atuantes na persecução penal, mesmo dentro de todas as normas de um Estado democrático e constitucional de Direito se denota uma linha de pensamento que se afasta do ponto de vista da filosofia da linguagem de Wittgenstein e da teoria da ação comunicativa de Habermas[103], e, por consequência, também da teoria do Professor Vives Antón (obviamente, respeitados os direitos e garantias fundamentais constitucionais dos cidadãos).

Sobre os malefícios de sequer se ter a possibilidade de produção probatória legítima de conversas criptografadas a fim de se examinar o sentido e o contexto havido entre os interlocutores, relevantes os seguintes trechos da obra Investigações filosóficas[104], dos quais atribuo pontos semelhantes, análogos, ainda que inexatos, ao caso-problema da E2EE:

> §246: Até que ponto as minhas sensações são privadas? – Bem, só eu posso saber se realmente tenho ou não uma dor; **uma outra pessoa só pode fazer uma conjectura. – Isto é, por um lado, falso, e por outro destituído de sentido**. (p. 336-337);
>
> §155 [...] no tribunal pode ter que se tratar da questão de determinar com que **intenção** é que uma palavra foi dita. E isto pode ser questão de intenção. Do mesmo modo, pode considerar-se **significativa** a maneira como uma pessoa viveu uma certa palavra [...]. (p. 577; grifo nosso).

Veja-se que a prova digital dotada de tecnologia incapaz de conhecimento por terceiros torna, para estes, uma ação inexistente, um sem sentido, ausente a linguagem como conhecimento à produção de um significado para terceiros que não

---

[103] "Habermas alerta: **essas formas de comunicação dependem da tecnologia da comunicação e para serem completas os sujeitos devem se descortinar do véu da tecnocracia e apresentar-se como seres humanos.** [...] avanços tecnológicos que em sua ideia originária seriam integradores sociais criam espaços de exclusões." (BETTINE, Marco. **A teoria do agir comunicativo de Jüger Habermas**: bases conceituais. São Paulo: EACH, 2021. 1 E-book, p. 87; grifo nosso).

[104] WITTGENSTEIN, Ludwig. **Tratado lógico-filosófico**. **Investigações Filosóficas**. Tradução e Prefácio: M. S. Lourenço. 6. ed. Lisboa: Fundação Calouste Gulbenkian, 2015.

fazem parte desta ação comunicativa, no caso, o Estado, representado pelos agentes de persecução penal legitimamente constituídos para o exercício desta função de controle na prática de crimes.

Essa crise na produção da prova penal digital demonstrada nos capítulos anteriores, e, a consequente pressão de várias Nações sobre as *Big Techs* pela quebra da criptografia por algum meio alternativo, pode se embasar por uma questão universal do ponto de vista não só do Direito (interceptação telemática devidamente motivada por um juízo competente), portanto, mas também, da filosofia da linguagem, em especial, na reunião de diversos pensadores da teoria da ação significativa:

> Este *sentido* de uma ação deve ser buscado no pensamento do segundo Wittgenstein, para quem, tal sentido surge da interação social mediada por regras, cuja inteligibilidade só é possível no contexto de uma *forma de vida* comum. As formas de vida comuns permitem-nos entendermo-nos acerca dos usos costumeiros de uma palavra para significar algo e para que uma ação seja identificada como tal, bem como para identificar de que tipo de ação se trata.
> Neste ponto, resulta decisiva a contribuição de Habermas, com sua teoria da ação comunicativa, tomada por Vives Antón para o desenvolvimento da chamada teoria da ação significativa.
> A ação se identifica não pela ideação ou pela consecução de um fim, mas sim pela característica de *seguir uma regra*, que é de onde deriva a expressão de *sentido* que permite diferenciar as ações dos meros acontecimentos como expressão de intenções, pretensões e propósitos. Claro está que estes só ganham existência no contexto de sua realização.[105]

Em suma, a "ação deve ser entendida [...] não como o que as pessoas *fazem*, mas como o *significado do que fazem*, ou seja, como o sentido de um substrato"[106]. E

> o ponto de partida é a **existência de um comportamento humano concreto e determinado**. Esse comportamento deve ser cotejado com as normas jurídicas. E, sobre esse comportamento concreto, devem ser projetadas todas as exigências contidas na lei penal para vincular uma consequência (pena), ou seja, comprovado que satisfaz todas as exigências das normas vigentes aplicáveis para poder puni-lo.[107] (Grifo nosso).

Como defendia o Professor Vives Antón, *"a linguagem privada é impossível"*, pois "para que haja linguagem, deve haver um mundo externo e vários sujeitos"[108],

---

[105] PRAZERES, Ângela dos; BUSATO, Paulo César. Heterorresponsabilidade e autorresponsabilidade penal de pessoas jurídicas: especial referência ao fato de conexão. In: BUSATO, Paulo César; GRECO, Luís (Coord.). **Responsabilidade penal de pessoas jurídicas**: anais do III seminário Brasil-Alemanha (v. 2, 2019, Berlin). Florianópolis: Tirant lo Blanch, 2020. p. 20-21.

[106] GONZÁLEZ CUSSAC, José Luis; BUSATO, Paulo César; CABRAL, Rodrigo Leite Ferreira. **Compêndio de direito penal brasileiro**: parte geral. Valencia: Tirant lo Blanch, 2017. p. 187.

[107] *Ibid.*, p. 190, grifo nosso.

[108] VIVES ANTÓN, Tomás S. **Fundamentos do sistema penal**. Tradução: Paulo César Busato. 2. ed. São Paulo: Tirant lo Blanch, 2022. p. 351.

impossibilitado, como regra, no caso da mensagem criptografada[109] e do ponto de vista do Estado, a aplicação da norma penal e processual penal constitucionalmente legitimadas.[110]

Consequentemente, a responsabilidade penal da pessoa jurídica dos provedores desses serviços de mensageria eletrônica criptografados de ponta a ponta, tal como pretende legislar os Estados Unidos da América, em breve aqui exposto, é uma resposta, ao menos formalmente, legítima a uma situação inédita de um processo de ausência de conhecimento possível pelo Estado de fatos penalmente relevantes, por conta de uma evolução tecnológica nas mãos das pessoas jurídicas de direito privado.

Possível uma releitura constitucional dos limites à interceptação telemática[111], mas não se mostra acertado um agir sem limites de fronteiras (globalização comunicativa), sejam para os interlocutores, seja para as próprias empresas que almejem se valer de países que os isentem de ordens judiciais em sentido oposto a alguma decisão judicial democraticamente produzida. Seria o setor privado sobrepondo-se aos interesses constitucionalmente previstos, discordantes ou não por parcela da sociedade, de uma Nação. Lembre-se, ademais, que não há princípio constitucional absoluto, e, a interceptação telefônica tem força normativa constitucional.

Diante de tudo isso, certamente a concepção significativa da ação deve ser somada aos argumentos para se solucionar o problema proposto nesta pesquisa científica em face do conflito de direitos e garantias fundamentais na produção da prova penal digital dotada da E2EE, avaliada no caso concreto:

> De fato, nos Estados Unidos, várias controvérsias afetam o status dos direitos do *bill of rights*, especialmente a relativa à admissibilidade ou inadmissibilidade de direitos constitucionais implícitos e a referente ao caráter material ou estritamente procedimental da cláusula *Due Process of Law*, tão

---

[109] Do segundo Wittgenstein: "O **significado da linguagem** é dado pelas regras que fazemos uso", permitindo que os indivíduos "**se relacionem com o mundo** [...] no **processo de significação**" (grifo nosso). Cf.: COSTA, Leandro S. Algumas considerações sobre a possibilidade de um enfoque antropológico na filosofia de Ludwig Wittgenstein. **Espaço Acadêmico**, Maringá, v. 15, n. 179, abr. 2016, p. 59.

[110] Ora, "Não tendo como distinguir entre enunciados verdadeiros ou falsos em relação a questões de fato, **se torna impossível fundamentar o conhecimento empírico nos dados dos sentidos**" (grifo nosso. Cf.: SALATIEL, José Renato. Filosofia analítica: Wittgenstein e o argumento da linguagem privada. **UOL**. Disponível em: https://educacao.uol.com.br/disciplinas/filosofia/filosofia-analitica-wittgenstein-e-o-argumento-da-linguagem-privada.amp.htm. Acesso em: 8 jul. 2022).

[111] Vide, conforme subcapítulo 3.1.2, o caso Jones v. United States, da Suprema Corte dos EUA.

> relacionada com a anterior e com o problema geral da interpretação da Constituição e, com ela, das liberdades básicas, que discorre em termos da oposição entre ativismo e *self-restraint*. Habermas, que se ocupou do papel e a legitimidade da jurisprudência constitucional nos Estados Unidos quanto na Alemanha, chega à conclusão que a escolha entre uma opção e outra **não pode ser feita em abstrato**, sem fornecer nenhum critério claro para levá-la a cabo, além da referência genérica ao papel da teoria do discurso.[112]

Por outro lado, e daí a dificuldade no julgamento por nossa Suprema Corte ADPF 403 e ADI 5527, enfatizava o Professor Vives Antón, quando tratava do dilema permanente entre a segurança material e a liberdade, que mesmo numa sociedade de risco global não se pode justificar o discurso do lema da lei e ordem, limitando-se a liberdade em nome da segurança, sob o pretexto utópico da "falsa crença da maioria de que a perda da liberdade é indiferente, porque afetará apenas os outros"[113]. Assim,

> Na "sociedade de risco global", as ameaças são tantas e tão graves que o papel que o Direito Penal pode desempenhar na sua prevenção e repressão, obviamente, é mínimo. Portanto, parece absolutamente inadequado reduzir as consequências na análise de risco de Beck a mudanças dogmáticas e político-criminais com as quais, diminuindo ou reduzindo as garantias, pretenda-se controlar a nova situação por meio do Direito Penal.[114]

No Brasil, deve ser evidenciado para fins de futura regulação legislativa, que a Constituição Federal (artigos 173, § 5º[115]; e, 225, § 3º[116]) não limitou os casos de responsabilidade penal de pessoa jurídica às hipóteses normativas hoje existentes (crimes ambientais, contra a ordem econômica e financeira e a economia popular)[117],

---

[112] VIVES ANTÓN, Tomás S. **Fundamentos do Sistema Penal**. Tradução: Paulo César Busato. 2. ed. São Paulo: Tirant lo Blanch, 2022, p. 806.

[113] *Ibid.*, p. 834.

[114] *Ibid.*, p. 835.

[115] Art. 173, § 5º: "A lei, sem prejuízo da responsabilidade individual dos dirigentes da pessoa jurídica, estabelecerá a **responsabilidade desta**, [...] nos **atos praticados contra a ordem econômica e financeira e contra a economia popular"** (BRASIL. Constituição da República Federativa do Brasil de 1988. **Diário Oficial da União**, Brasília, DF, 5 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 8 jul. 2022).

[116] Art. 225, § 3º: "As condutas e atividades consideradas lesivas ao **meio ambiente** sujeitarão os infratores, pessoas físicas ou **jurídicas**, a sanções penais e administrativas, independentemente da obrigação de reparar os danos causados" (*Ibid.*).

[117] SYDOW, Spencer Toth. Curso de direito penal informático. 2. ed. Salvador: Juspodivm, 2021, p. 86: atualmente, "Não há qualquer previsão para a responsabilização criminal da pessoa jurídica em matéria penal informática". Destaca o autor que o art. 21 do Marco Civil da Internet trata da responsabilidade civil das empresas de tecnologia.

dado seu rol exemplificativo[118], o que, aliado à Convenção de Budapeste (o seu art. 12, item 3, prevê a possibilidade de responsabilidade penal da pessoa jurídica a ser legislada pelo Estado-parte), independentemente do resultado das ações constitucionais em trâmite no STF, é mais um indício de uma mudança anunciada no âmbito da abertura de um dever legal do setor privado na produção da prova penal digital, mesmo dotado de uma tecnologia criada que, ao menos em tese e de forma geral, impede qualquer ingerência por terceiros que não os próprios interlocutores.

Como esse rol da Constituição Federal brasileira não é taxativo quanto ao âmbito de imputação delitiva, e, ao mesmo tempo, nem todos os crimes são possíveis de serem realizados por empresas, destacam-se sugestões[119] oportunas ao estudo desta dissertação quanto ao papel e responsabilidades das plataformas digitais (*providers*): a previsão legal de crimes com a expressão "realizados por ela" (p. 65), e, a independência da responsabilidade da pessoa jurídica a de seus dirigentes (pessoas físicas) pela prática de delitos "compatíveis com sua natureza e capacidade de realização" (p. 65), deixando em aberto aos hermeneutas e juristas o uso destas duas soluções à possibilidade de imputação a delitos já existentes e, também, a outros futuros.

No âmbito prático dessa relação público-privado, portanto, a criação de uma nova tecnologia pelo particular (E2EE), aliado a algum meio que permita ao Estado a produção da prova penal digital com tal criptografia, dentro de limites normativos diferenciados e sob certas responsabilidades das pessoas jurídicas, parece ser o caminho intermediário de um agir democrático, cooperativo e, por conseguinte, de maior efetividade à resposta ao problema.

Veja-se que há dois alertas, das conclusões de Vives Antón a respeito dos ensinamentos do jurista Julius H. von Kirchmann[120] sobre a Ciência do Direito, que se

---

[118] "A comissão elaboradora do projeto de Código penal optou [...] por interpretar que a referência constitucional à responsabilidade penal de pessoas jurídicas é meramente exemplificativa, sendo permitida sua distensão para outros campos" (BUSATO, Paulo César. Razões criminológicas, político-criminais e dogmáticas para a adoção da responsabilidade penal de pessoas jurídicas na reforma do Código Penal brasileiro. In: BUSATO, Paulo César; GUARAGNI, Fábio André. **Responsabilidade penal da pessoa jurídica**: fundamentos criminológicos, superação de obstáculos dogmáticos e requisitos legais do interesse e benefício do ente coletivo para a responsabilização criminal. Curitiba: Juruá, 2012. 1ª Reimp.: 2013. p. 53-54).

[119] *Ibid.*, p. 65.

[120] Cf.: Reivindicación del pensamento de un fiscal prusiano. In: VIVES ANTÓN, Tomás S. **Pensar la libertad**: últimas reflexiones sobre el derecho y la justicia. Compiladora: María Luia Cuerda Arnau. Valencia: Tirant lo Blach, 2019. p. 625-640.

adequam à celeuma da E2EE e à produção da prova penal digital: a observância do princípio da legalidade e as razões de uma justiça universal democrática voltada à efetividade e resolução de casos concretos, como corolários inerentes a tal finalidade probatória. Em suma: a) "As famosas três palavras do legislador que arruínam bibliotecas inteiras" [121] não indica crítica de Kirchmann à lei positiva, mas somente, uma inadequação comparativa de estudo da ciência do Direito às ciências naturais; b) "A aplicação do procedimento generalizador que, a semelhança do que se usa nas ciências, remonta a ideias ou princípios cada vez mais abstratos, resulta destrutiva no âmbito do direito, cujo objetivo é resolver conflitos singulares" [122], ou seja, devemos nos afastar do generalismo, da ideia de verdades últimas, e, sob a cautela de que "nossa razão subjetiva não procede imparcialmente, senão guiada por interesses particulares, que muitas vezes utilizam a abstração como modo de ocultar" [123].

Desse modo, os desafios das pulsantes novas tecnologias são inerentes ao realismo social e a reação é também a alteração das normas e dos julgados (como se verificará no capítulo seguinte). Os serviços de comunicação social pelo meio digital universalizados aceleraram a forma como todo o sistema jurídico deve se adaptar, inclusive do ponto de vista de uma necessária observância de precedentes de casos semelhantes como matéria inerente à motivação de votos que tratam do mesmo assunto (sob pena de incongruência fática), pelo enriquecimento de argumentos e, da aplicação da Convenção de Budapeste, sem prejuízo de outros acordos e tratados internacionais, não só no caso brasileiro, mas também de dezenas de Nações democráticas que aderiram a este tratado internacional.

Nesse mesmo sentido, esclarece a doutrina as repercussões diversas que, no Brasil, as decisões advindas dos tribunais internacionais podem ocorrer; uma delas, de função argumentativa ou persuasiva, não vinculante, como a ora proposta:

> Portanto, [...] os tribunais brasileiros estão livres para considerar o peso, ainda que o peso decisivo, das decisões precedentes de órgãos internacionais ou mesmo estrangeiros, por conta da persuasão de sua fundamentação – tanto quanto ponderam sobre o valor de material doutrinário ou de jurisprudência interna, em geral, e desde que consideradas as diferenças sistemáticas e culturais.
> Vale lembrar que, em relação às decisões dos órgãos internacionais aos quais o Brasil se vinculou, não há ponderação: trata-se de jurisprudência com

---

[121] *Ibid.*, p. 630, tradução nossa.
[122] *Ibid.*, p. 630.
[123] *Ibid.*, p. 631.

> caráter normativo, a ser observado e reconhecido no direito brasileiro, por força do sistema constitucional brasileiro.[124]

Assim sendo, a partir de caso prático em discussão atual por todo o planeta sobre a interceptação telemática em comunicações digitais protegidas pela criptografia ponta a ponta em investigações criminais, é possível transpassar o pensamento bitolado de que o julgamento da Suprema Corte nacional pode ser dado como fundamento último, ou por si só, sem considerar o arcabouço que se traz de outras Nações democráticas, em direção a um fundamento plural, propondo sua análise não como regra de forma vinculativa aos julgados, mas, como complemento em matéria preliminar, ou, no próprio exame de mérito do voto do julgador[125], no mínimo, por seu valor argumentativo.

A busca de fundamentos plurais[126], portanto, das mais variadas fontes, é o mote do capítulo seguinte.

---

[124] ALLE, Saulo Stefanone. **Produção probatória e cooperação jurídica internacional em matéria penal.** Revista Brasileira de Ciências Criminais, São Paulo, v. 156, p. 425-452, jun. 2019, DTR\2019\31676, p. 16.

[125] Cf.: COSTA, Daniel Tempski F. da. **O pós-fundacionalismo como fundamento de uma nova técnica de decisão judicial em casos de repercussão globalizada**: a força dos precedentes estrangeiros no julgamento interno em defesa de um pluralismo jurídico democrático. In: SOUZA NETTO, José Laurindo; GIACOIA, Alberto; CAMBI, Eduardo (Coord.). Direito, **gestão** e **democracia**: estudos em homenagem ao Ministro Felix Fischer. Curitiba: Clássica, 2022, p. 115-131).

[126] E, "a colocação de uma única solução global, para os diversos desafios que surgem com a temática da guerra cibernética, gera o desconforto da imposição de soluções arbitrárias", buscando-se um remédio democrático e ciente de uma pluralidade normativa. Cf.: BARROS, Renata Furtado de. Guerra cibernética: os novos desafios do direito internacional. Belo Horizonte: D'Plácido. 2021, p. 166.

3 O TRATAMENTO JURÍDICO VIGENTE E PROPOSTO DA CRIPTOGRAFIA PONTA A PONTA COMO FUNDAMENTO DO ESTUDO DO DIREITO COMPARADO

3.1 ESTADOS UNIDOS: A MUTAÇÃO CONSTITUCIONAL DA 4ª EMENDA, OS NOVOS PROJETOS DE LEI E A RELEVÂNCIA DAS *BIG TECHS* NO DEBATE PELA REGULAÇÃO DA E2EE

Nos Estados Unidos, a 4ª emenda de sua Constituição dispõe sobre a proibição da busca e apreensão sem que haja motivo razoável, ou, de maneira desarrazoada (*reasonableness clause*), através de mandado judicial baseado em causa provável (*warrant clause*), com a delimitação da suficiente descrição do local dessa cautelar de busca e das coisas a serem apreendidas.[127]

A doutrina, há décadas, analisa sucessivas releituras sobre a interpretação e aplicação desse preceito constitucional norte-americano (as garantias da 4ª emenda[128]), com supedâneo em diversos julgados, que indicam uma evolução necessária para conciliar tal redação aos novos tempos, especialmente, o uso da tecnologia nos meios de comunicação digital na investigação criminal[129].

Importante destacar que o termo "mutação normativa" (constitucional, no caso) pode ser utilizado como sinônimo de "evolução na interpretação", alerta que ora se faz para estancar alguma dúvida por eventual confusão no uso equivalente de tais expressões. Dos ensinamentos do constitucionalista alemão Peter Haberle, conforme artigo do Ministro Gilmar Ferreira Mendes (em coautoria), tem-se que:

> **a norma, confrontada com novas experiências, transforma-se necessariamente em uma outra norma.** [...] Daí a necessidade de, em tais

---

[127] Tradução: "O direito do povo de estar seguro em suas pessoas, casas, papéis, e bens pessoais, contra desarrazoadas buscas e apreensões, não será violado, nem mandados poderão ser expedidos, senão baseados em causa provável, suportada por juramento ou afirmação, e particular descrição do local a ser buscado e das pessoas e coisas a serem apreendidas". Disponível em: https://www.britannica.com/topic/Fourth-Amendment. Acesso em: 22 set. 2021.

[128] O termo "***effects***", da 4ª emenda, significa "bens pessoais", como acima traduzido, o que inclui telefones celulares, computadores, veículos (v.g.: localização por GPS e leitura de placas, especialmente) e todos os outros artigos de propriedade móvel, ponto chave neste estudo.

[129] Há o reconhecimento no STF da mutação constitucional em face da evolução das novas tecnologias de armazenamento de dados nos telefones celulares, como a necessidade de autorização judicial para a verificação de conversas em aplicativo WhatsApp. (In: BRASIL. Supremo Tribunal Federal. Habeas Corpus n. 168.052/SP, 2ª Turma. Relator: Min. Gilmar Mendes, Brasília, 02 dez. 2020; grifo nosso).

> casos, fazer-se o ajuste do resultado, adotando-se técnica de decisão que, tanto quanto possível, traduza a **mudança de valoração**. No **plano constitucional**, esses casos de mudança na concepção jurídica podem produzir uma **mutação normativa ou a evolução na interpretação**, permitindo que venha a ser reconhecida a inconstitucionalidade de situações anteriormente consideradas legítimas.[130] (Grifo nosso).

No Brasil, há escasso estudo detalhado da origem histórica da 4ª emenda[131], apesar da relevância e de menções como fonte de direito comparado em diversos julgados na Suprema Corte[132] de nosso país[133] de doutrina e jurisprudência dos Estados Unidos[134]. Também sobre a importante "Teoria do Mosaico", evidenciada em precedentes dos EUA, tampouco se encontram julgados brasileiros por sua aplicação expressa após extensa busca em diversos *sites*, exceto por citação tangente do termo "mosaico probatório" ou, em direito civil, sobre a classificação "famílias mosaico".[135]

Diante disso, será traçada uma linha histórica de julgados emblemáticos da Suprema Corte dos EUA, com a finalidade de demonstrar as mudanças quanto ao alcance da 4ª emenda, basicamente, decorrentes da evolução da tecnologia utilizada nas investigações criminais. Com isso, objetiva-se corroborar quais linhas interpretativas de sua atual aplicação são possíveis e os seus limites constitucionais para a efetiva persecução criminal, garantindo os direitos dos cidadãos diante de ações policiais, mas, ao mesmo tempo, sem esquecer da segurança pública e da

---

[130] MENDES, Gilmar Ferreira; VALE, André Rufino do. A influência do pensamento de Peter Häberle no STF. **Conjur**, abr. 2009, p. 7. Disponível em: https://www.conjur.com.br/2009-abr-10/pensamento-peter-haberle-jurisprudencia-supremo-tribunal-federal?pagina=7. Acesso em: 18 nov. 2021).

[131] Conforme prefácio da renomada Professora Lêda Boechat Rodrigues em: RAMOS, João Gualberto Garcez. **Curso de Processo Penal Norte-Americano**. 2. ed. No Prelo.

[132] O STF aplicou, expressamente, a 4ª emenda dos EUA, ao estender o direito à privacidade em busca e apreensão de computadores usados por servidores públicos dentro da repartição governamental, com duas exceções: "consentimento (renúncia) do titular ou por ordem judicial". Cf.: BRASIL. Supremo Tribunal Federal. Habeas Corpus n. 132.062/RS, 1ª Turma. Relator: Min. Marco Aurélio; Relator do Acórdão: Ministro Edson Fachin. Brasília, 22 nov. 2016.

[133] Há outras citações expressas da 4ª emenda dos EUA no STF, v.g.: RE 522897 (rel. Min. Gilmar Mendes); e ADI 6387 MC (rel. Min. Rosa Weber).

[134] A influência do direito norte-americano e alemão nos Acórdãos do STF, alerta a doutrina, impõe cuidado em razão de alguns exemplos malsucedidos. Vide: BORGES, A. O direito estrangeiro no aperfeiçoamento da jurisdição constitucional brasileira. **Jota**, nov. 2021. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/penal-em-foco/direito-estrangeiro-jurisdicao-constitucional-brasileira-16112021. Acesso em: 19 nov. 2021.

[135] Em buscas jurisprudenciais por "teoria" e "mosaico", acesso em 10 out. 2022, nenhuma trouxe na forma da doutrina norte-americana do caso Jones; o primeiro *site* busca julgados do STF, STJ, todos os TRF's, suas TR's e a TNU; e, o segundo, também os TJ's estaduais, além dos antes mencionados: BRASIL. Conselho da Justiça Federal. Disponível em: https://www2.cjf.jus.br/jurisprudencia/unificada; *Idem*. **Jusbrasil**. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/busca?q=%22mosaico%22+%22teoria%22&p=3.

efetividade da justiça penal, evitando-se a produção de provas ilícitas, processos natimortos.

3.1.1 Linha temporal das alterações do alcance da 4ª emenda

Do surgimento da doutrina do castelo (*castle doctrine*) da Inglaterra do Séc. XVIII até sua implantação e constante releitura da 4ª emenda nos EUA, verifica-se que a abrangência desta passou da mera análise dos limites físicos, corpóreos, tangíveis da casa ("castelo") do investigado, ou de seu patrimônio.

No caso **Olmstead v. United States**, julgado em **1928**, a Suprema Corte dos EUA decidiu que não houve violação à 4ª emenda, pois a escuta telefônica foi instalada pela polícia em um poste público, na calçada, fora da propriedade do acusado. E, de igual maneira, em **Goldman v. United States (de 1942)**, a Suprema Corte não considerou inconstitucional a escuta telefônica feita pelo FBI, porquanto a polícia usou um aparelho que se acoplava à parte externa da parede do escritório do investigado de crime.

Porém, no julgamento do caso **Katz v. United States (1967)**, em nova interpretação, voltou-se o pensamento jurídico interpretativo para algo incorpóreo[136], notadamente, a intimidade, a privacidade do cidadão, independentemente de tal limitação física, resultando no chamado **"teste de Katz"**, termo que vem sendo utilizado pela doutrina e jurisprudência norte-americana desde então[137]. Do precedente, extrai-se que foi concretizada

> a consciência de que **a forma restritiva de ver o problema – apenas vinculado à invasão física dos espaços particulares – não resolveria nenhum problema relevante colocado pela persecução penal**. A decisão, nesse caso, foi no sentido de que a atividade de espionagem por parte do Estado viola uma **'expectativa de privacidade'** do imputado, que confiou justamente estar se comunicando ao telefone sem que ninguém o estivesse escutando. [...] A opinião da Corte termina assim: **Concluímos que [...] a doutrina da invasão não pode ser considerada como a que controla a admissibilidade dessas provas em juízo. As atividades estatais de escuta eletrônica e gravação das palavras do imputado violaram a privacidade sobre a qual ele justificadamente confiou ao falar ao**

[136] RAMOS, p. 116-117. No prelo.

[137] O juiz Harlan, em Katz, estabeleceu o teste para as proteções da 4ª emenda: "quando uma pessoa [exibe] uma expectativa real (subjetiva) de privacidade, e [quando] a expectativa" é a sociedade reconhece ser razoável." (In: KUGLER, Mattew B.; STRAHILEVITZ, Lior. Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory. **The Supreme Court Review**, Chicago, 2015, p. 213. Disponível em: bit.ly/3FuqHI40. Acesso em: 08 jul. 2021).

> **telefone e, assim, devem ser consideradas 'busca e apreensão' no sentido da 4ª emenda. O fato de que o equipamento eletrônico não ultrapassou os muros da propriedade do imputado não tem significação constitucional**.

Veja-se que[138]

> **Katz erigiu a expectativa de privacidade em critério para detectar uma violação por parte do poder público**. Se a atitude do imputado, ao realizar uma comunicação captada pela autoridade pública, revelar que esperava, razoavelmente, ter privacidade, então a autoridade violou seus direitos da 4ª emenda. **Se, por outro lado, o imputado realizar uma comunicação em público – por exemplo, gritar para um comparsa em um local movimentado –, entende-se que abriu mão voluntariamente de sua privacidade**. Será legítima a captação dessa comunicação. **A expectativa de privacidade do imputado, por outro lado, também deve ser legítima**, isto é, deve ser de molde a ser aceita pelo conjunto da sociedade. Em outras palavras, **não há legítima expectativa de privacidade para a prática de atividades ilícitas.** (Grifo nosso)

Reafirmou-se o teste de Katz quando a Suprema Corte dos EUA considerou ilegal a prova por ser irrazoável o uso pela polícia, **sem mandado judicial**, de **dispositivo de imagem térmica** para detectar atividade dentro da casa do investigado, medindo o calor mesmo que do lado de fora, em nome da garantia de privacidade da 4ª emenda. A regra concebida nesse julgado para limitar o uso policial de novas tecnologias as quais podem "reduzir o domínio da privacidade garantida" é que, ao obter a informação relativa ao interior da casa que de outra forma não poderia ter sido obtida sem material físico, houve uma **intrusão em uma área constitucionalmente protegida, constituindo-se uma busca pelo uso de tecnologia que não é de uso do público geral, e**,

> Reverter **essa abordagem deixaria o proprietário à mercê do avanço da tecnologia,** incluindo a tecnologia de imagem que poderia discernir **todas** as atividades humanas em casa. Também rejeitada é a alegação do governo de que a imagem térmica era constitucional porque não detectou "detalhes íntimos". Tal abordagem seria errada em princípio porque, na santidade do lar, todos os detalhes são detalhes íntimos .[139] (Tradução e grifo nossos).

---

[138] Cf.: RAMOS, João Gualberto Garcez. **Curso de Processo Penal Norte-Americano**. São Paulo: Revista dos Tribunais, 2006, p. 131.

[139] SUPREME COURT OF THE UNITED STATES. Kyllo v. United States, 533 U.S. 27, 2001. Disponível em: https://supreme.justia.com/cases/federal/us/533/27. Acesso em: 11 nov. 2021.

Verifica-se, destarte, que a mutação constitucional[140] é inevitável quanto ao alcance da 4ª emenda, naturalmente, em face da sua inalterada redação desde 1791[141] e ocorre constante necessidade da sua releitura por legítimos interesses, apesar de antagônicos.

Desde o caso Katz aos dias atuais, a transformação global da sociedade, interligada pela *internet*, trouxe a necessidade de uma resposta do Direito (ainda longe de pacificação) a demandas inevitáveis trazidas pela tecnologia, especialmente, quanto ao seu uso nas investigações criminais e suas intercorrências, positivas e negativas, aos direitos e garantias fundamentais. Os valores democráticos estão em debate por todo o mundo por razão dessa celeuma. Pretende-se o resguardo da privacidade e intimidade de um lado, e, por outro, do interesse público voltado ao combate à criminalidade, ambos com excelentes razões de existência.

O uso constante de *smartphones* com informações – fotos, vídeos, mensagens, *e-mails* – da vida privada quase completa dos cidadãos, telecomunicações criptografadas de ponta a ponta, câmeras com monitoração 24 horas dirigida a alguma casa, leitura de placas de veículos nas vias públicas (ALPRS – *Automated license plate readers*), *drones* dotados de câmeras de vigilância noturna, enfim, uma infinidade de meios tecnológicos são o novo desafio das Nações para dar conta de uma releitura constitucional da 4ª emenda, sem perder de vista o devido processo legal para dar efetividade no combate à criminalidade, a qual, de igual maneira, utiliza-se da tecnologia para seus objetivos ilícitos.

Com isso, dá-se um salto na linha do tempo da história para os precedentes jurisprudenciais que modificaram o alcance da 4ª emenda por essa influência tecnológica, cada uma com fundamentos novos, naturais da constante alteração não só do caso em concreto, mas de uma necessidade decorrente das mudanças sociais em alta velocidade.

3.1.2 Jones *v.* United States (2012) e a aplicação implícita da Teoria do Mosaico

---

[140] A visão do Direito que prega a busca pelo significado original, mascara preferências políticas conservadoras, "como é o caso do originalismo norte-americano (POST; SIEGEL, 2016, p. 492)" Cf.: DIAS, Eduardo R.; ROCHA, Robert F. A Constituição líquida: mutação constitucional e expansão de direitos fundamentais na hipermodernidade. **Direitos Fundamentais e Democia**, Curitiba, v. 24, n. 1, jan./abr. 2019. DOI: 10.25192/issn.1982-0496.rdfd.v24i11423.

[141] RAMOS, p. 27. No prelo.

As manifestações sobre essa problemática advinda das novidades tecnológicas e sua influência gigantesca na esfera privada dos cidadãos repercutiram nos Estados Unidos no caso **Jones v. United States** (julgado em 2012).

A Suprema Corte norte-americana firmou entendimento de que, em face das novas tecnologias, acrescentou-se algo de novo quanto ao alcance da 4ª emenda, criando interpretação mais abrangente que o juízo anterior do que se pode esperar por análise limitada à "expectativa razoável de privacidade" (o chamado "teste de *Katz*")[142], pelo acesso quase que integral à vida dos cidadãos norte-americanos ao se ter acesso ao *smartphone* (ou outros meios tecnológicos de possível extensa vigilância da vida privada).

Isso porque foi utilizado como fundamento desse caso a denominada Teoria do Mosaico[143], a fim de se considerar a soma de informações privadas obtidas do cidadão como um todo, não de forma isolada, e, assim, verificar, no caso em concreto, se cabível a aplicação dos ditames da 4ª emenda[144].

O fato objeto de discussão em Jones v. United States[145] diz respeito ao rastreamento de rota do carro de um investigado, o réu Antoine Jones, por tráfico de drogas pela polícia, mas a destempo e noutra localidade (ou seja, depois do período autorizado de 10 dias do mandado judicial de busca e apreensão anteriormente deferido, para o distrito de Columbia), ao se instalar um GPS (quando estacionado em estacionamento público e na parte debaixo do carro) por 28 dias (após o 11º dia e noutro distrito, de Maryland; portanto, com erro de execução pela polícia, como se estivesse ausente de autorização judicial), o que configurou uma busca a ser analisada se dentro das garantias da 4ª emenda pelo Judiciário.

---

[142] Em: SUPREME COURT OF THE UNITED STATES. Katz v. United States, 389 U.S. 347, 1967. Disponível em: https://supreme.justia.com/cases/federal/us/389/347. Acesso em: 07 jun. 2021.

[143] O reexame do tema sobre a Teoria do Mosaico será explanado de forma mais detalhada no subcapítulo 3.1.5.

[144] Do voto da Magistrada JJ. Sotomayor: "pode ser necessário reconsiderar a premissa de que um indivíduo não tem nenhuma expectativa razoável de privacidade em informações voluntariamente divulgadas a terceiros", uma abordagem que ela considerava "mal adequada à era digital" (SUPREME COURT OF THE UNITED STATES. United States v. Jones, 2012. Disponível em: https://www.law.cornell.edu/supct/pdf/10-1259.pdf. Acesso em: 07 jun. 2021; p. 19).

[145] Corroborado pela doutrina: "**As opiniões em Jones, assim, abrem a porta para uma Quarta Emenda mais expansiva**", dada a aplicação da Teoria do Mosaico (cf.: SLOBOGIN, Christopher. Making the Most of United States v. Jones in a Surveillance Society: A Statutory Implementation of Mosaic Theory. **Duke Journal of Constitutional Law & Public Policy**, n. 8, p. 1-37, 2012. Disponível em: http://scholarship.law.duke.edu/djclpp/vol8/iss1/1. Acesso em: 07 jun. 2021; p. 4).

Em resumo, por maioria de votos (6 votos a 5), entendeu a Suprema Corte ter havido violação à 4ª emenda, em destaque ao seu vocábulo "*effects*", mesmo com a decisão anterior do Tribunal Distrital de ter suprimido os dados GPS obtidos enquanto o veículo estava estacionado na residência de Jones, mantidos os dados restantes como prova (informações do GPS conectavam Jones ao esconderijo dos supostos conspiradores, onde havia U$ 850.000 em dinheiro, 97 kg de cocaína e 1 kg de base de cocaína), porque Jones não tinha "expectativa razoável de privacidade" quando o veículo estava em vias públicas. Veja-se que, em seguida ao julgamento do Tribunal Distrital (grande Júri), o Tribunal de Apelações dos Estados Unidos para o Circuito do Distrito de Columbia reverteu a condenação por tráfico de drogas, por entender ter sido violada a 4ª emenda pelo uso sem justificativa do dispositivo GPS)[146].

Desse julgamento devem ser feitos importantes apontamentos.

O primeiro diz respeito ao grande passo para a era moderna quanto à resposta judicial ao uso das novas tecnologias utilizadas para a investigação policial. Julgou-se que haveria necessidade do mandado judicial em tal rastreamento via GPS ininterrupto por 28 dias pela elevada quantidade de atos reunidos ou agrupados (mais de 2 mil páginas de dados) extrapolar o razoável do que se espera da privacidade, pois, quando reunidos, tem-se uma linha enorme da vida privada do cidadão (tal como o conceito da Teoria do Mosaico[147]) pela exposição de seus trajetos e paradeiros. Por consequência, revelaram-se dados exagerados da sua intimidade e estranho ao objeto de investigação, com base nas diversas informações expressas e lógicas decorrentes do referido mosaico de dados, configurando violação desarrazoada de seus direitos tutelados pela 4ª emenda. O veículo foi entendido como um "bem pessoal" ("*effects*") desta emenda e, para instalar o GPS, decidiu-se que a polícia invadiu a propriedade do investigado, já que expirado o prazo e local diverso do mandado judicial.

O segundo apontamento pertinente do julgado é que todos os magistrados, apesar de algumas divergências noutros pontos de suas motivações, concordaram

---

[146] SUPREME COURT OF THE UNITED STATES. United States v. Jones, 132 S. Ct. 945, 2012. Disponível em: https://www.law.cornell.edu/supremecourt/text/10-1259. Acesso em: 28 set. 2021.

[147] SLOBOGIN, *Op. cit*, p. 24-25: "nem a Juíza Sotomayor, nem o Juiz Alito, tentam explicar como essa teoria [Mosaico] pode ser implementada. [...] O professor Orin Kerr, que não é fã da teoria do mosaico, compilou [...]: (1) Que teste determina quando um mosaico foi criado? (2) Como a vigilância não contínua deve ser analisada? (3) Quais técnicas de vigilância são regidas pela teoria do mosaico? (4) Que nível de justificativa é necessário para realizar uma busca em mosaico?".

em afastar a denominada ***third-party doctrine*** (doutrina de terceiros)[148]: a controversa noção de que os funcionários do governo não precisam de justificativa sob a Constituição para ver ou acessar quaisquer atividades ou informações que possam ser vistas ou acessadas por terceiros "fora da casa", isto é, o fato de que terceiros podem observar o veículo quando em via pública não é irrelevante diante da quantidade enorme de dados privados obtidos, quando reunidos nesses 28 dias.

Destarte, antes do caso Jones, embasadas na doutrina de terceiros, defendia-se que as investigações governamentais semelhantes não estavam sob a égide da 4ª emenda, indicando abuso de poder em face dos cidadãos norte-americanos, tais como: a tecnologia ligada a carros, GPS (Jones); sinais de telefones (localização do usuário); câmeras de vigilância (*zoom*, rastreamento e reconhecimento facial); *drones* sobrevoando áreas específicas para filmagem; acesso a computadores (dados pessoais, cartões de crédito, transações bancárias, *e-mails*, registros de telefone)[149]. Exemplos que, exceto no caso Jones (GPS instalado no veículo do investigado), não há sequer uma invasão física de propriedade (*trespass*), daí a iniciativa policial sem mandado.

Em terceiro, como fundamento do caso, não se abandonou o teste de Katz ("expectativas razoáveis de privacidade") na análise. A Juíza Sotomayor enfatizou ter ocorrido uma busca ilícita, pois ausente mandado judicial válido e não houve o consentimento do réu. E, o juiz Alito, no que acordou a juíza Sotomayor, ponderou que situações envolvendo meramente a transmissão de sinais eletrônicos sem invasão permaneceriam sujeitas à análise de Katz. Observe-se que o Estado recorrente admitiu o descumprimento do mandado e argumentou apenas que ele não era necessário.

Por fim, entendeu-se que o critério da duração do ato policial (longo tempo da investigação por GPS, e, consequentemente, de elevada quantidade de dados

---

[148] Quanto à "regra polêmica de que a informação perde proteção da Quarta Emenda quando é revelada conscientemente a um terceiro", os estudiosos "**têm [a] atacado repetidamente [...] com base no fato de que não é convincente em sua aparência e dá ao governo muito poder**" (KERR, Orin S. The Case for the Third-Party Doctrine. **Michigan Law Review**, v. 107, n. 561, Feb. 2009. p. 9 – tradução e grifo nossos. Disponível em: bit.ly/3FuUXCy. Acesso em: 28 set. 2021).

[149] SLOBOGIN, *Op. cit*, p. 2 (tradução e grifo nossos): "**A decisão em Jones está muito atrasada. Governos federais, estaduais e locais estão rapidamente aproveitando os avanços tecnológicos para manter o controle sobre seus cidadãos, de maneiras cada vez mais intrusivas**. [...]. Antes de Jones, a doutrina de terceiros garantiu que nenhuma dessas atividades fosse regulamentada pela Quarta Emenda".

privados obtidos) para decidir pela inconstitucionalidade das provas obtidas, não devem ser levados como critério certo e derradeiro em casos futuros, pois podem haver ocorrências de vigilância de curta duração, mas com resultado enorme de informações colhidas.

Pelo exposto, o acesso a informações, quase ilimitadas na vida das pessoas, resultou em novo alcance da proteção da 4ª emenda. Os juízes da Suprema Corte[150] endossaram o que a Corte inferior de Jones chamou de Teoria do Mosaico[151], ou seja, um incremento do que se tinha anteriormente como delineado na proteção constitucional da 4ª emenda, com consequências jurídicas muito discutidas por seus juízes, principalmente a necessidade de uma legislação para melhor disciplina do tema[152], evitando-se buscas e apreensões ilícitas, prisões arbitrárias, abuso de poder e, consequentemente, a inefetividade da justiça penal por posteriores anulações de julgamentos.

Além disso, o uso da Teoria do Mosaico, ao invés da motivação de análise do caso utilizar-se somente do teste de Katz e da mera análise individual (de forma isolada) e sequencial de cada um dos atos investigados, mesmo criticada pela doutrina, resultou em precedentes judiciais nas instâncias inferiores, e também bastante divergentes. Mais um indicativo da necessária regulamentação legal pelos estados norte-americanos[153], como enfatizado pelo juiz Alito no julgamento do caso

---

[150] SLOBOGIN, *Op. cit*, p. 3-4, grifo nosso: "Em suma, ambas as opiniões [juíza Sotomayor e juiz Alito] endossaram o que a Corte inferior de Jones chamou de **"teoria do mosaico" da Quarta Emenda** – a ideia de que certos tipos de investigação governamental permitem o acúmulo de tantos bits individuais sobre a vida de uma pessoa que o quadro de personalidade resultante é digno de proteção constitucional. [...] Mas a Corte ainda tem muito o que resolver. [...]."

[151] "**Antes de Jones, as decisões da Quarta Emenda sempre avaliavam cada etapa de uma investigação individualmente**. Jones introduziu [a] "teoria do mosaico" [que] reflete preocupações legítimas, mas implementá-la seria extremamente difícil à luz das rápidas mudanças tecnológicas" (KERR, Orin S. The Mosaic Theory of the Fourth Amendment. **Michigan Law Review**, v. 111, n. 3, p. 311, 2012 – tradução e grifo nossos).

[152] Há, assim, críticas quanto à implementação prática da Teoria do Mosaico, mediante inúmeros questionamentos (quanto à aplicabilidade e ambiguidade de conceitos jurídicos indeterminados). Contudo, como se verá nos pontos seguintes, recentemente **tal teoria foi, ainda que implicitamente, reafirmada pela Suprema Corte no caso Carpenter (2018).** Ademais, juízos de grau inferior já vêm utilizando de tal interpretação, e, novas leis vêm surgindo nos EUA.

[153] Os "efeitos multiplicadores de um processo de regulamentação faz com que a polícia estenda as regras sobre atividades ainda não determinadas judicialmente como "buscas e apreensões", que ajudariam os tribunais a fazer essas determinações sem produzir consequências prejudiciais ao desempenho policial." (AMSTERDAM, Anthony G. Perspectives on the Fourth Amendment. **Minnesota Law School**, n. 848, 1974, p. 75. Disponível em: bit.ly/3h5rXba. Acesso em: 20 out. 2021.

Jones[154]; e, já em 1974, pelo renomado professor emérito da Universidade de Nova Iorque, Anthony Amsterdam, quando enaltecia as garantias da 4ª emenda e defendia, para a eficiente investigação policial, a necessária criação de normas prévias às buscas e apreensões para controle de atos ilegais, auxiliando também o Judiciário na proteção constitucional. Em destaque, tem-se uma recente legislação aprovada no estado de Utah, que será analisada em subcapítulo próprio desta dissertação.

3.1.3 O caso Riley *v.* Califórnia (2014)

Pouco tempo depois, em 2014, do julgamento de Jones v. United States, em **Riley v. California**[155], decidiu-se, por unanimidade, que a busca e apreensão, sem mandado judicial, de conteúdo digital de um telefone celular durante uma prisão, é, via de regra, inconstitucional. A exceção: alguma "circunstância exigente" (perigo iminente) diante de uma prisão legal. E, neste ponto, merece uma pausa na exposição do julgado para explicar o que se entende nos EUA, segundo abalizada doutrina[156], por tais circunstâncias exigentes, as quais são lembradas em muitos julgados como "exceções "de perigo" à 4ª emenda[157], de segurança nacional[158] ou perecimento de provas imediatas:

> Circunstâncias exigentes: **(a)** Circunstâncias que sugerem um perigo grave e específico, nesse caso **é permitida uma busca** se um oficial da lei acreditar que é razoável e necessário ajudar a evitar o **perigo percebido**; ou **(b)** circunstâncias envolvendo **perigo iminente ou desaparecimento de provas que dificultem a obtenção de um mandado ou ordem judicial** em tempo hábil, nesse caso apenas causa provável ou suspeita razoável, como o caso pode ser, é necessária antes da busca. [...] A subseção (a) implementa a

---

[154] SLOBOGIN, *Op. cit*, p. 36-37: "as legislaturas são mais bem equipadas do que os tribunais, vinculados como são pelo caso [...], para fornecer regulamentos detalhados e abrangentes sobre uma ampla gama de cenários".

[155] SUPREME COURT OF THE UNITED STATES. Riley v. California, 573 U.S. 373, 2014. Disponível em: https://supreme.justia.com/cases/federal/us/573/373. Acesso em: 06 jun. 2021.

[156] Conforme: SLOBOGIN, *Op. cit*, p. 23, tradução e grifo nossos.

[157] Abrem-se portas, todavia, à criticada política investigativa governamental pela **NSA** (National Security Agency) no dilema de escusa em nome da defesa nacional e ausência de ordem judicial, principalmente após os ataques terroristas do 11 de setembro de 2001. Vide: ACLU. **NSA spying on americans is illegal**. Disponível em: https://www.aclu.org/other/nsa-spying-americans-illegal. Acesso em: 25 nov. 2021.

[158] Há preocupações legítimas: "na Síria, estão recrutando [...] americanos problemáticos para matar pessoas, [usando] **aplicativos de mensagens móveis de ponta a ponta criptografadas, comunicações que não podem ser interceptadas, apesar das ordens judiciais ao abrigo da Quarta Emenda**." (Tradução e grifo nossos. HARVARD UNIVERSITY. **Don't Panic: Making Progress on the "Going Dark" Debate**. Cambridge, 2016. Disponível em: bit.ly/3Hb8ocg. Acesso em: 16 nov. 2021, p. 7).

> **exceção de perigo** [...]. Destina-se a abranger **crises de segurança nacional e outras emergências significativas, iminentes ou não.** Subseção (b) é uma definição padrão de exigência focada em **saber se há tempo para obter uma ordem**. Subseção (a) é a única reverência **à sugestão do juiz Alito em Jones de que as técnicas investigativas normalmente regidas pela Quarta Emenda não devem estar sujeitas à regulamentação constitucional quando usadas para investigar "crimes extraordinários".** Caso contrário, essa definição de circunstâncias exigentes não relaxa as restrições às buscas com base na natureza do delito. Essa posição baseia-se no pressuposto de que **a busca de provas de um crime já cometido não merece menos regulamentação simplesmente porque o crime é grave**.

Observe-se que a Suprema Corte brasileira já vem aplicando tal conceito[159] em casos envolvendo a busca e apreensão domiciliar, o que corrobora sua importância e o estudo do direito comparado como algo imperativo:

> A proteção contra a busca arbitrária **exige que a diligência seja avaliada com base no que se sabia antes de sua realização, não depois.**
> Esse princípio é **adotado pelo direito norte-americano**, na medida em que não dispensa o mandado em situações de crime em curso, salvo se a busca imediata decorrer de circunstâncias exigentes – **"exigent circumstances" – , assim consideradas "as circunstâncias que levariam uma pessoa razoável a crer que a entrada era necessária para prevenir o dano aos policiais ou outras pessoas, a destruição de provas relevantes, a fuga de um suspeito, ou alguma outra consequência que frustre indevidamente esforços legítimos de aplicação da lei"** – [...]" [United States v. McConney, 728 F. 2d 1195, 1199 (9th Cir.), cert. denied, 469 U.S. 824 (1984)].

Depois desse necessário recorte, já que utilizado o termo "circunstâncias exigentes" não só neste julgado, mas também em diversos pontos desta dissertação, imperativo o retorno à explanação do caso Riley.

Inicialmente, deve-se sublinhar que, na verdade, apesar do chamativo jurisprudencial e doutrinário, o exame da matéria constitucional pela Corte máxima americana abrangeu dois casos concretos distintos (acusados de nomes Riley e Wurie).

No precedente nº 13-132, relativo ao peticionário Riley, este foi detido por uma infração de trânsito, o que acabou levando-o à prisão por porte de arma, quando então um policial apreendeu seu celular do bolso da sua calça, e, acessando as informações do telefone, averiguou o uso repetido de um termo associado à gangue de rua; duas horas depois, já na delegacia, um detetive especializado em gangues examinou o conteúdo digital do telefone e, com base nas fotos e vídeos encontrados, o Estado

---

[159] STF. Plenário. Recurso Extraordinário 603.616, relator Ministro Gilmar Mendes, julgado em 05 nov. 2015, p. 19-20.

acusou Riley da autoria de um tiroteio ocorrido semanas antes de sua prisão e buscou a sua condenação com fulcro em tais provas obtidas via celular, **ausente de mandado judicial**. O réu se insurgiu para suprimir todas as evidências que a polícia havia obtido de seu telefone celular, mas o tribunal de origem negou a moção de Riley, o qual foi condenado. Este resultado, contudo, após o julgamento pela Suprema Corte, foi revertido e remetido ("*reversed and remanded*") ao grau inferior de jurisdição.

Já no julgado sob nº 13–212, o acusado Wurie foi preso depois que a polícia o observou participando de uma aparente venda de drogas e só então, na delegacia, os policiais apreenderam o celular de Wurie; em seguida, os policiais rastrearam o número de uma chamada que estava recebendo, nominada como "minha casa". Suspeitando ser o apartamento do preso, a polícia **obteve um mandado judicial de busca** e, ao final, encontraram drogas, uma arma de fogo, munição e dinheiro. Wurie foi então acusado de delitos de drogas e armas de fogo, e tentou suprimir as evidências obtidas na busca no apartamento junto ao tribunal distrital, o qual negou a moção de Wurie, restando condenado. A Suprema Corte manteve o julgado ("*affirmed*").

A Corte Constitucional, em suma, afastou as teses do governo-recorrente, confirmando que não são casos de exceção às garantias da 4ª emenda a análise do celular do preso, com base nos seguintes motivos: **a) a busca de informações digitais em um telefone celular não promove os interesses do governo identificados em Chimel**[160] (no julgado *Chimel v. Califórnia*, exigiu-se que um incidente de busca para prisão fosse limitado à área dentro do controle imediato do detido, justificado em nome da segurança do policial e na prevenção da destruição de provas) **e implica interesses de privacidade individual substancialmente maiores do que uma breve busca física**, porquanto os dados do celular não podem colocar o policial em perigo e seu exame externo é garantido (arma, droga no aparelho); **b)** os Estados Unidos e a Califórnia levantaram **preocupações sobre a destruição de evidências**, argumentando que, mesmo que o telefone celular seja fisicamente seguro, as informações no telefone celular permanecem vulneráveis à **limpeza remota e criptografia de dados**; porém, a Corte afastou tal tese, tendo como

[160] Supreme Court of the United States. Chimel *v.* California, 1969: "Um oficial que faz a prisão pode revistar o preso para descobrir e remover armas e apreender evidências para evitar sua ocultação ou destruição, e pode fazer uma busca na área "dentro do controle imediato" da pessoa presa, ou seja, a área de onde ele pode obter a posse de uma arma ou evidência destrutível" (Disponível em: https://supreme.justia.com/cases/federal/us/395/752. Acesso em: 15 out. 2021).

argumentos serem essas alegações **genéricas** e **distintas do foco do precedente Chimel**, no qual o preso tentou ocultar ou destruir, efetivamente, as evidências ao seu alcance, e, além disso, as forças de segurança possuem **tecnologia para combater a perda de evidências** (limpeza remota); **c)** os interesses de privacidade do celular são mais substanciais (no sentido quantitativo, pelo número de informações do cidadão, e qualitativo, pela natureza de dados praticamente completas de todos os aspectos da vida privada) comparados a outros objetos de posse do preso, sobressaindo-se ao interesse do Estado como regra (numa referência, indireta, da **Teoria do Mosaico**); **d)** por último, foram **afastadas as propostas alternativas do governo** da possibilidade da: **(1)** busca sem mandado no celular de um preso quando "fosse razoável" acreditar que o telefone tivesse evidências do crime da prisão ocorrida, momento em que a Corte motivou que essa proposta não é adequada neste contexto (celular) e não se revelaria nenhum limite prático quando se trata de buscas de telefones celulares, pois tem acesso a muitas informações (privacidade), e acabaria legitimando sempre a busca sem mandado; **(2)** estabelecer regra possível em restringir o escopo de uma busca pelo telefone celular a informações relevantes sobre o crime, a identidade do preso ou a segurança do policial; todavia, essa proposta imporia poucas restrições significativas aos policiais quanto ao acesso ao aparelho; **(3)** o estado da Califórnia sugeriu uma regra analógica, segundo a qual os oficiais poderiam pesquisar dados de telefones celulares se pudessem obter as mesmas informações de uma contraparte pré-digital (registros físicos – ex.: mera agenda de nomes), contudo, também este requerimento foi afastado, porque permitiria que os agentes da lei pesquisassem uma ampla gama de itens contidos em um aparelho, mesmo que as pessoas não carregassem tanta variedade de informações na forma física, e lançaria aos tribunais difícil delimitação fática para determinar quais arquivos digitais são comparáveis aos registros físicos.

É de se destacar parte importante do julgado, indicando clara diferença na obtenção de dados nos telefones celulares que há pouco tempo atrás e, diante disso, a necessidade da releitura quanto ao alcance da 4ª emenda:

> Mas os telefones celulares podem armazenar milhões de páginas de texto, milhares de fotos ou centenas de vídeos. Isso tem **várias consequências de privacidade inter-relacionadas.** Primeiro, um telefone celular coleta em um lugar muitos tipos distintos de informações que **revelam muito mais em combinação do que qualquer registro isolado**. Em segundo lugar, a capacidade do telefone permite que apenas um tipo de informação transmita muito mais **do que era possível anteriormente**. Terceiro, os dados do

> telefone podem **remontar há anos**. Além disso, um elemento de difusão caracteriza os telefones celulares, mas não os registros físicos. Uma década atrás, os policiais podem ter ocasionalmente tropeçado em um item altamente pessoal, como um diário, mas hoje muitos dos **mais de 90% dos adultos americanos que possuem telefones celulares mantêm consigo um registro digital de quase todos os aspectos de suas vidas**[161] (tradução e grifo nossos).

Para estancar qualquer dúvida, ponderou o Juiz-Chefe de Justiça da Suprema Corte norte-americana, John Roberts, que a "resposta à pergunta sobre o que a polícia deve fazer antes de revistar um telefone celular apreendido de forma incidente quando da prisão é simples: obtenha um mandado" [162].

A Corte máxima norte-americana, afastando as teses do governo, reconheceu que essa limitação exposta no caso concreto impactará na atividade policial, mas deixou claro que **não obstou seja feito, por mandado judicial, a busca no telefone celular**, sugerindo maior cuidado e eficiência na expedição destes dada a importância da 4ª emenda. Vale de novo frisar, ademais, que foi deixada uma brecha: não afastaram a possibilidade de **exceção** à 4ª emenda (desnecessidade de mandado) em casos de "circunstâncias exigentes"[163].

3.1.4 Carpenter *v.* United States (2018)[164] e a Teoria do Mosaico "em duas etapas"

No caso **Carpenter v. Estados Unidos**, a Suprema Corte anunciou, em resumo, que através de informações históricas de localização obtidas via celular (*cell site location information* – CSLI**,** via dados de empresas provedoras de serviços sem fio, como a AT&T e a T-Mobile, por triangulação de torres de telefonia celular), conseguiu-se precisar a localização do acusado Timothy Carpenter (peticionário da

---

[161] SUPREME COURT OF THE UNITED STATES. Riley v. California, 573 U.S. 373, 2014. Disponível em: https://supreme.justia.com/cases/federal/us/573/373. Acesso em: 05 jun. 2021.

[162] THE SUPREME COURT – LEADING CASES. Fourth Amendment – Search and Seizure – Searching Cell Phones Incident to Arrest – Riley v. California. **Harvard Law Review**, v. 128, n. 251, 2014, p. 253. Disponível em: https://harvardlawreview.org/wp-content/uploads/2014/10/riley_v_california.pdf. Acesso em: 02 nov. 2021).

[163] *Idem*, p. 253: "O Tribunal, portanto, evitou cautelosamente o atoleiro legal representado pelos programas de **metadados da NSA**". A NSA faz parte do Departamento de Defesa dos EUA, e faz uso "de um sistema chamado de Signals Intelligence (SIGINT), que é capaz de obter **interceptações e criptoanálise** de sinais" (NASCIMENTO, Anderson. **O que é a NSA**. Disponível em: https://canaltech.com.br/espionagem/O-que-e-a-NSA. Acesso em: 4 nov. 2021).

[164] SUPREME COURT OF THE UNITED STATES. Carpenter v. United States, 585 U. S. 2018. Disponível em: https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf. Acesso em: 07 jul. 2021.

demanda). Chegou-se a quatro locais da presença de Carpenter, num raio de 3km dos locais dos roubos, pelo que foi acusado e preso pela autoridade policial; essa "busca" foi realizada pela polícia **sem mandado** baseado nas exigências da 4ª emenda, mas com fulcro na *Stored Communications Act* (ato normativo anterior à era da internet[165]), que possui demanda valorativa reduzida (inferior) de privacidade, comparada à "causa provável" estabelecida nos termos da aludida exigência constitucional. Em suma[166]

> Além do CSLI, Carpenter apresenta uma oportunidade importante para o Tribunal revisitar o SCA [Stored Communications Act]. Escrito antes da era da Internet, esse estatuto é agora muito utilizado pelas autoridades não apenas para obter informações sobre telefones celulares, como o CSLI, mas também para obter acesso a informações relacionadas a e-mails e atividades online de provedores de serviços de Internet ("ISPs").

Decidiu a Corte Constitucional norte-americana que houve uma "busca" no sentido da 4ª emenda, ou seja, o caso exigia mandado judicial ("causa provável") com base fática-probatória mais robusta que a adquirida inicialmente. Aplicou-se, outrossim, e ainda que indiretamente[167], a Teoria do Mosaico ao motivar que uma série de ações governamentais devem ser entendidas como se fossem um todo, um agrupamento, desses atos separados; como se as pequenas peças informativas de geolocalização de vários dias formassem um único conjunto.

O acórdão traz como argumentos principais[168]: **a)** a 4ª emenda protege não apenas os interesses de propriedade, mas também certas expectativas razoáveis de privacidade; os precedentes da era fundadora (historicamente julgados pela Suprema Corte dos EUA) continuam a informar este Tribunal ao aplicar a 4ª emenda às **inovações** nas ferramentas de vigilância; **b)** o diferentecial, contudo, é que os **dados digitais** em questão (informações de localização pessoal mantidas por terceiros) **não se encaixam perfeitamente sob esses precedentes judiciais existentes, mas estão na intersecção de duas linhas de casos: b.1)** de um lado, aborda a

---

[165] LEGAL INFORMATION INSTITUTE (LII). **18 U.S. Code Chapter 121 – Stored Wire And Electronic Communications and Transactional Records Access**. Disponível em: https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121. Acesso em: 02 nov. 2021.

[166] MEYER, Jonathan E.; CARLSON, Sonja S. Supreme Court Reenters Fray on Privacy: Carpenter v. United States. **National Law Review**, June 2017. Disponível em: https://www.natlawreview.com/article/supreme-court-reenters-fray-privacy-carpenter-v-united-states. Acesso em: 02 nov. 2021.

[167] "De fato, os casos pós-Jones indicam que quase todos os juízes estão começando a falar sobre privacidade em termos de teoria do mosaico" (KUGLER; STRAHILEVIT, *Op. cit*, p. 208, tradução e grifo nossos).

[168] SUPREME COURT OF THE UNITED STATES. Carpenter... *Op. cit*, p. 1-4.

expectativa de privacidade de uma pessoa em sua localização física e movimentos registrados por GPS instalado em seu veículo (Jones v. Estados Unidos); **b.2)** e um outro, volta-se a uma expectativa de privacidade de uma pessoa em informações entregues voluntariamente a terceiros; **c)** a natureza singular dos registros de localização através do telefone celular, de forma contínua, levou a Suprema Corte à recusa em aplicar a "*third-party doctrine*": **c.1)** a Suprema Corte, já em Riley v. Califórnia, reconheceu que os indivíduos têm uma expectativa razoável de privacidade em toda a sua movimentação física e, assim, caso se permita ao governo acesso a registros de localização de celular estaria avesso a tal expectativa; **c.2)** o Governo, como parte recorrente, alegou que a doutrina de terceiros rege este caso, porque são "registros de negócios" criados e mantidos por operadoras de telefonia sem fio; contudo, tal argumento foi afastado, pois é incomparável aos precedentes arguidos (Smith e Miller)[169], já que as informações não são conscientemente compartilhadas pelo usuário com terceiros, mas são parte inerente do uso do serviço de telefonia (ocorre com o mero uso do aparelho), ou seja, não são compartilhadas pelo investigado, e fazem já parte inerente da participação na sociedade moderna seu difundido uso; **d)** deixa-se claro que a decisão é limitada ao caso concreto, revelando a instabilidade jurídica que os variados meios de investigação, mormente por novas tecnologias revelarem o quanto a resposta jurídica está sempre atrás dessas mudanças; o acórdao, portanto, é expresso que a decisão não altera eventual interpretação para a devida aplicação dos precedentes de Smith e Miller, ou, trata de outras técnicas e ferramentas de vigilância[170]; tampouco considera outras técnicas investigativas envolvendo relações exteriores ou de segurança nacional, aliás, este é um adendo que várias vezes se ressalva nas decisões, como nos casos Jones e Riley, quanto às "circunstâncias exigentes". Portanto, conclui-se, que se o Governo precisar de um mandado para acessar o CSLI, sob tal argumento excepcional, poderá haver uma busca sem mandado judicial.

---

[169] O "Tribunal considerou que um cliente não tem expectativa razoável de privacidade nos números de telefone que disca (Smith) e nos cheques e guias de depósito que entrega ao seu banco (Miller), pois os expôs a outro e, assim, assume o risco de serem entregues ao governo" (Tradução nossa). Disponível em: bit.ly/3utSoun. Acesso em: 08 nov. 2022. Cf.: THOMPSON II, Richard M. **The Fourth Amendment Third-Party Doctrine.** Congressional Research Service, June 2014, p. 2.

[170] Tal precedente corrobora a tendência de um rol exemplificativo, aberto, sobre as técnicas de investigação digital de mensagens dotadas de E2EE.

Verifica-se, assim, que se desenvolveu a partir desse caso um *plus* quando comparado ao caso Jones, porque refletiu uma nova abordagem para a Teoria do Mosaico, desenvolvida no subcapítulo a seguir.

3.1.5 Decorrências atuais da mutação constitucional da 4ª Emenda no ordenamento jurídico dos EUA

A compilação desses marcantes precedentes jurisprudenciais para se compreender a alteração do alcance da tutela da 4ª emenda no direito constitucional e processual penal dos Estados Unidos ao longo de sua história até as modificações inerentes que a tecnologia ocasionou em todo o mundo encabeçam novas situações relevantíssimas no ordenamento jurídico desse país. A **primeira**, quanto à visão crítica doutrinária a partir da jurisprudência na aplicação da Teoria do Mosaico e dos recentes julgados da Suprema Corte, sobretudo com a releitura no caso Carpenter. A **segunda**, a constatação de uma necessidade de atuação legislativa, decorrente de uma *obiter dictum* da Suprema Corte no caso Jones, que, apesar de argumento de passagem ou reforço, repercutiu fortemente no ordenamento jurídico norte-americano, a fim de se realizar uma equalização, em prol da segurança jurídica e da praticidade, ao tentar se adiantar as hipóteses abrangidas pelas novas tecnologias utilizadas na produção de provas[171].

Esses dois importantes pontos de análise serão dispostos em seguida, mas o alcance de suas conclusões deve influenciar ordenamentos jurídicos por todo o mundo dada a relevância digital dos Estados Unidos, sede de grandes empresas detentoras de tecnologia, além do cumprimento da Convenção de Budapeste, aderida por dezenas de países, inclusive o próprio EUA.

3.1.5.1 A Teoria do Mosaico em uma e em duas etapas e sua criticada aplicação nos tribunais norte-americanos

[171] Observação perspicaz é a do renomado jurista Mirjan Damaška, quanto à normatização superlativa, caso lembrados da vinculação por tal função normativa dos precedentes no sistema do *common law*, em especial, relativo à matéria probatória de seu livro ora reportado, ou seja, tanto quanto de uma lei formal (DAMAŠKA, Mirjan R. **Evidence Law Adrift**. New Haven: Yale University Press, 1997. p. 8-9).

Utilizando-se da continuidade do exame jurisprudencial dos EUA em face dos conflitos decorrentes da evolução tecnológica com as técnicas investigativas dos crimes comuns e dos novos surgidos (ditos cibernéticos[172]), merece pesquisa mais aprofundada da Teoria do Mosaico, pois já há certa releitura prática de aplicação nos tribunais inferiores norte-americanos do exame de diferentes tecnologias de investigação utilizadas na persecução criminal.

Como adendo, é preciso destacar a origem da Teoria do Mosaico na doutrina alemã, em 1972, voltada à proteção de dados privados[173]. Na época, logicamente, não se poderia imaginar a enorme relevância da aplicação atual quanto a aspectos processuais penais e de análise da garantia constitucional nos moldes da 4ª emenda dos EUA e para vários outros países pela utilização mundial da *internet* como meio cotidiano de vida, dado o inimaginável salto tecnológico da humanidade.

Também na Espanha, a partir da década de 70, ainda que timidamente, a Teoria do Mosaico[174] foi estudada do ponto de vista da proteção da garantia à intimidade[175] em razão dos avanços da informática[176]. Merece destaque tal abordagem histórica[177]:

> Por todas essas razões, postulou-se que a teoria das esferas deveria ser substituída pelo que **a primeira doutrina alemã de proteção de dados chamou de "teoria do mosaico"**. [...] é um avanço inquestionável para

---

[172] Do relatório do Projeto do novo Código Penal há a **classificação de crimes cibernéticos** "**próprios**" (relacionados com o sistema informático, protegendo-se sua confidencialidade, integridade e funcionamento) e "**impróprios**" (os de mera utilização de sistema informático como meio delitivo), conforme será visto no subcapítulo 4.3.

[173] SEIDEL, Ulrich. **Datenbanken und Persönlichkeitsrecht**: Unter besonderer Berücksichtignung der amerikanichen Computer Privacy. Köhl: O. Schmidt, 1972.

[174] Sobre as ultrapassadas teorias das esferas e do espiral para análise do limite à intimidade-privacidade, vide: MADRID CONESA, 1984 (apud MENDOZA, Melanie Claire F.; BRANDÃO, Luiz Mathias R. Do direito à privacidade à proteção de dados: das teorias de suporte e a exigência da contextualização. **Revista de Direito, Governança e Novas Tecnologias**, Brasília, v. 1, p. 223-240, 2016. Disponível em: https://www.indexlaw.org/index.php/revistadgnt/article/view/830. Acesso em: 10 out. 2021.

[175] Sobre a Teoria do Mosaico (*Idem*, p. 10): "Existem dados a priori irrelevantes do ponto de vista do direito à intimidade e que, todavia, em conexão com outros, talvez também irrelevantes, podem servir para fazer totalmente transparente a personalidade do cidadão, como ocorre com as pequenas pedras que formam os mosaicos, que em si não dizem nada, mas que unidas podem formar conjuntos plenos de significados" (tradução nossa).

[176] Há um terceiro conceito de direito à intimidade, de Madrid Conesa: a Teoria do Mosaico, surgida à sua proteção **"frente às ameaças dos novos engenhos tecnológicos [**...] **a informática"**. (tradução e grifo nossos – VOLPATO, Samira. **El Derecho a la Intimidad y las Nuevas Tecnologias de la Información**. Tesis (Doctorado en Derecho Constitucional) – Universidade de Sevilla, Sevilla, 2016. p. 54. Disponível em: https://idus.us.es/handle/11441/52298. Acesso em: 07 jul. 2021.

[177] HUERTA, Pablo Pascual. **La génesis del derecho fundamental a la protección de datos personales**. Tesis (Doctorado en Derecho Constitucional) – Universidad Complutense de Madrid, Madrid, 2017, p. 212-213. Disponível em: https://eprints.ucm.es/id/eprint/43050/1/T38862.pdf. Acesso em: 10 nov. 2021).

> enfocar corretamente as ameaças causadas pela informatização, enquadra-se perfeitamente na essência da informática e da teoria da informação: **a informação não é definida por seu conteúdo, mas por sua quantidade. Na Espanha**, pelo contrário, é preciso esperar vários anos para ver uma contribuição equivalente a estes. As obras que tratam do tema na década de 70 podem ser contadas nos dedos de uma mão. (Tradução e grifo nossos).

O ressurgimento dessa teoria em território norte-americano, portanto, décadas depois, mais que mera constatação doutrinária, revela a importância do estudo da história do Direito através de seus precedentes e do direito comparado a uma entrega jurisdicional dentro do devido processo legal. E o seu emprego aparece agora como solução que já está se enraizando pelos tribunais dos EUA e, com certeza, serão de extrema valia nos tribunais brasileiros para o exame constitucional de (i)licitude das provas penais digitais.

Desse modo, num segundo momento de apreciação jurisdicional de casos concretos no dia a dia forense, surgiu uma outra leitura de como proceder ao uso da Teoria do Mosaico, inerente e interligada às novas tecnologias disponíveis, seja para uso pessoal, como os *smartphones*, seja para uso da polícia às investigações criminais ou voltadas à segurança pública investigativa, preventiva e repressiva (*drones*, filmagens em via pública de pessoas e veículos, CSLI etc.), inclusive de forma crítica quanto à retenção abusiva de informações pelo governo respaldada, justamente, mas sob outra perspectiva, por essa teoria.

Nesta seara, por um outro aporte crítico diferenciado quanto à utilização da Teoria do Mosaico, tem-se o alerta pela eventual forma abusiva do governo para justificar a limitação do acesso público a dados secretos que obtêm dos cidadãos, sob o argumento de que os terroristas podem **superlativizar dados que isoladamente não são importantes, mas que ao serem agrupadas o serão**, tendo como pano de fundo "a luta contra o terror", mormente após os ataques de 11 de setembro (EUA) e diante das novas tecnologias, resguardando, destarte, a retenção de informações pela jurisprudência norte-americana sob essa outra perspectiva, do sigilo estatal justificado[178].

Destarte, como delineado no exame dos precedentes judiciais do capítulo anterior, a alteração do raciocínio jurídico embasado na Teoria do Mosaico surgiu de

---

[178] Cf.: POZEN, David E. The Mosaic Theory, National Security, and the Freedom of Information Act. **The Yale Law Journal**, v. 115, n. 628, 2005, p. 631 e 632. Disponível em: https://core.ac.uk/download/pdf/157778843.pdf. Acesso em: 12 nov. 2021. Veja-se: "o escopo da atividade oficial agora está sendo protegido pela teoria do mosaico; [...] os tribunais têm respaldado deferência às agências [...] de maneiras [...] suscetíveis a abusos e excessos" (*Ibid.*).

forma natural, por necessidade de resposta jurídica a um modo de vida da sociedade atual, regida de forma inerente em seu cotidiano pelas novas tecnologias, desde o citado caso Jones até o precedente Carpenter.

Em seguida, a doutrina, embasada na jurisprudência não só da Suprema Corte, mas de vários tribunais de grau inferior dos EUA, entendeu ter havido uma subdivisão na forma de análise da Teoria do Mosaico, preconizando que no caso Jones se fez uso dessa teoria em uma etapa (*one-step*), e em Carpenter, em duas etapas (*two-steps*), quanto à avaliação dos dados digitais serem merecedores ou não, uma vez agrupados, de proteção sob a 4ª emenda, defendendo-se mais satisfatória a aplicação da teoria quando feita em duas etapas em relação a de uma só, tal como o exemplo do caso Carpenter.[179]

Em síntese, preconiza a doutrina[180] que, diante da análise das **decisões dos tribunais inferiores,** a Teoria do Mosaico em **duas etapas de Carpenter** fornece uma maneira de avaliar esses dados melhor que o de uma etapa de Jones, por **considerar o tipo de informação revelada e, em seguida, aplicar os fatos do caso** e, ademais, permite que os tribunais fundamentem os motivos que certas informações devem ser protegidas ou não, impedindo a ossificação da doutrina da 4ª emenda no campo da vigilância digital, a qual muda rapidamente.

Assim, ao invés de se analisar, de uma só vez, como no caso Jones, todos esses dados do mosaico informativo obtido na investigação dos dados arrecadados, verifica-se, primeiramente, a **natureza** da informação ou dados (**primeira** etapa), ou seja, se tem o **potencial** de, por si só, invadir a esfera razoável de privacidade do acusado com base em fatos específicos do caso concreto, e então, somente passada esta etapa com uma resposta afirmativa, passa-se à **segunda** etapa: o julgador deve verificar se a **quantidade** de dados ou informações agregadas (mosaico) como prova dos autos, **efetivamente**, invadiram a privacidade do investigado de forma desarrazoada.

---

[179] Em Carpenter, por primeiro, a Suprema Corte se concentrou na natureza das informações que a CSLI transmitiu antes de considerar o valor arrecadado na causa, ou seja, se esses dados, considerados de forma agrupada ou agregados tiveram o potencial de violar uma expectativa razoável de privacidade; e, depois, verificou-se, no caso concreto, se as informações obtidas do investigado assim o fizeram.

[180] WILSON, Taylor H. The Mosaic Theory's Two Steps: Surveying Carpenter in the Lower Courts. **Texas Law Review Online**, v. 99, n. 155, 2021, p. 182. Disponível em: https://texaslawreview.org/wp-content/uploads/2021/04/Wilson_Final_Read_2-1.pdf. Acesso em 12 nov. 2021 (grifo nosso).

Os exemplos jurisprudenciais de tribunais inferiores após os casos Jones e Carpenter, do uso da Teoria do Mosaico de uma e duas etapas, são vários. Esclarecem os julgados tal forma de aplicação usando a tecnologia como ponto de partida da análise de possível violação da 4ª emenda, como a da vigilância por câmeras de vídeo conectadas a uma central que realizam a leitura de placas de veículos automatizados (ALPRS), que por elas passam, apontando sua localização, data e hora que o motorista passou pelo trecho da via pública (similar ao caso Carpenter quanto ao CSLI, portanto). Em suma, a depender do caso em concreto (número de câmeras, tempo de vigilância e vezes que o motorista passou por elas), podem tais registros revelar um padrão na vida íntima do cidadão e demonstrar a violação, ou não, da 4ª emenda, necessitar, ou não, da autorização judicial dentro do devido processo legal.

No caso **Chaney v. Cidade de Albany**, utilizou-se a Teoria do Mosaico de uma etapa. Julgou-se que o uso de câmeras fixas, as quais gravavam, de forma indiscriminada, 24 horas por dia, não era uma busca abarcada pela 4ª emenda, pois esse uso específico capturou apenas informações sobre pessoas "viajando em vias públicas" e as pessoas não têm uma expectativa razoável de privacidade neste espaço público. No mesmo sentido em **Uhunmwangho v. Estado [Texas]**, pois aqui a polícia havia recuperado "uma única fotografia" do réu "dirigindo em uma via pública, o que, obviamente, nem de perto levanta preocupação de reunião de dados ou informações para uma expectativa mínima de invasão na intimidade do investigado[181].

Outros tribunais, contudo, aplicaram a Teoria do Mosaico em duas etapas, como em **Estados Unidos v. Yang**, em que a polícia consultou um banco de dados ALPR para encontrar um fugitivo, mas, apesar de o juiz Carlos Bea ter motivado que há possibilidade de os ALPRs apresentar os problemas, em tese, de Carpenter, dada a reunião de volumosas informações de forma automática da localização do veículo do investigado, isto é, de violar uma expectativa razoável de privacidade (padrão Katz), eles não o fizeram no caso então em julgamento, porque a consulta ao banco de dados "não revelou a totalidade, ou mesmo nenhum, dos movimentos físicos do réu".[182]

---

[181] Cf.: WILSON, *Op. cit*, p. 171.
[182] *Op. cit. Ibid.*, p. 172.

Logo, mesmo com alguma crítica doutrinária[183] e divergente forma de aplicação pelos tribunais da Teoria do Mosaico, ela já está enraizada no ordenamento jurídico norte-americano[184], oferecendo vantagens na análise judicial de uma possível verificação de violação da 4ª emenda, pois "os juízes podem resolver as disputas diante deles, deixando a porta aberta para futuros desenvolvimentos tecnológicos – exatamente o que o Tribunal fez em Carpenter"[185].

E a complexidade após a inserção da Teoria do Mosaico, apesar de necessária em face da antiga base interpretativa do teste de Katz não dar mais conta, sozinha, das novas tecnologias, demanda uma sistematização prévia e regrada que os tribunais não possuem, daí a prevista ideia de legalização formal pelo juiz Alito.

Aliás, uma tendência de regulação legislativa desse imbróglio jurídico quanto às novas tecnologias e o direito penal e processual penal revela-se necessária neste assunto, tal como se verifica concretizar-se por países de todo o mundo[186], exemplificativamente, os projetos de lei dos Estados Unidos e do Brasil, como na própria Convenção de Budapeste.

Essa releitura da 4ª emenda pelos tribunais de grau inferior, pouco tempo depois do caso Jones, decorrente de diversos julgamentos por todo os Estados Unidos, demonstra a necessidade de lei para uniformizar a matéria, estruturando o trabalho policial e o controle judicial.

Mesmo assim, como vemos da prática forense brasileira, ocorre a produção de provas ilícitas; porém, a legalização tem vantagens, como maior segurança jurídica (ainda maior se promulgada lei no mesmo sentido de precedentes formados pela Suprema Corte), e, principalmente, clarificação de regras prévias e gerais para abarcar uma gama enorme de novos meios de obtenção de provas em razão das crescentes distintas tecnologias utilizadas nos meios de investigação, formas de

---

[183] Cite-se: FAIRBANKS, R. Masterpiece or Mess: The Mosaic Theory of the Fourth Amendment Post-Carpenter. **Berkeley Journal of Criminal Law**, v. 26, n. 1, p. 71-119, 2021. Disponível em: https://doi.org/10.15779/Z38DZ03287. Acesso em: 14 nov. 2021. Aqui, prefere-se a norma, sem prejuízo da via jurisprudencial, mas em segundo plano: "O legislador pode [...] alterá-la ou eliminá-la diretamente, ao contrário do longo processo de recurso do judiciário" (p. 115, Tradução nossa).

[184] Nesse sentido, favorável à Teoria do Mosaico: "Orin [Kerr] acha que a teoria é falha. Eu concordo – mas é melhor do que as alternativas" (ROSENZWEIG, Paul. In Defense of the Mosaic Theory. **Lawfareblog**, Nov. 2019. Disponível em: https://www.lawfareblog.com/defense-mosaic-theory. Acesso em: 08 jul. 2021.

[185] WILSON, *Op. cit*, p. 179.

[186] Nos Estados Unidos isso será demonstrado em seguida, mas o interesse é mundial, como citado em diversas passagens deste trabalho.

controle de produção e exame de admissibilidade de provas, visando ao equilíbrio das demais garantias constitucionais, para evitar alegação de nulidade.

Nesse sentido, recentemente, o estado de Utah disciplinou parte do tema, conforme exame mais à frente.

3.1.5.2 A produção legislativa disciplinadora da 4ª emenda em face das novas tecnologias: uma necessidade anunciada pela Suprema Corte dos EUA

No julgamento do caso Jones v. United States[187] pela Suprema Corte norte-americana já se antevia, dada a complexidade da matéria (ofensa à 4ª emenda em face das novas tecnologias digitais de informação), a necessidade de uma legislação regulando-o, como levantando pelo juiz Alito da Suprema Corte dos EUA. No Brasil, esta é a regra[188], o que, de certa forma, contrapondo-se à análise do direito comparado[189], percebem-se vantagens, como a contenção de abusos policiais, controle de atos judiciais e a não surpresa em matéria probatória, privilegiando-se, ainda que por contraditório diferido, a paridade de armas com a Defesa; isso evita, na medida do possível, julgamentos anulados por prova ilícita.

Assim, o caminho da produção legislativa é uma realidade, inclusive em países que adotam o *common law*, como os EUA e o Reino Unido[190], mediante atos de força do governo com a bandeira midiática do abuso sexual infantil. Mas, como se perceberá, em ambos os países se ataca, ainda que implicitamente, a criptografia de ponta a ponta.

---

[187] E desde antes, genericamente, já se enfatizava "a força anglo-americana para legalizar questões probatórias" (p. 1924). Cf.: FRIEDMAN, Richard D. Anchors and Flotsam: Is Evidence Law 'Adrift'? Review of Evidence Law Adrift, by M. R. Damaška. **Yale Law Journal**, v. 107, n. 6, 1998. Disponível em: https://repository.law.umich.edu/reviews/14. Acesso em: 05 nov. 2021.

[188] Nos EUA, dado o *common law,* "a decisão de uma corte federal dizendo que a lei autoriza o FBI a conduzir um certo tipo de vigilância é muito valiosa" (PFEFFERKORN, Riana. O debate estadunidense sobre vigilância e criptografia. In: ANTONIALLI, Dennys; ABREU, Jacqueline de Souza (Ed.). **Direitos fundamentais e processo penal na era digital**. São Paulo: InternetLab, 2018. v. 1. Disponível em: bit.ly/3VW64df. Acesso em: 11 nov. 2021, p. 122).

[189] Os EUA aumentaram sua produção legislativa e o *civil law* deve confiar nos precedentes para preservar a "coerência" do Direito – Cf. KOZICKI, Katya; PUGLIESE, William S. Uma era de common law para o Brasil? In: Congresso Internacional de Direito Constitucional e Filosofa Política, 2., 2015: Belo Horizonte, MG; In: BUSTAMANTE, Thomas et al. (Org.). **Precedentes judicias, judicialização da política e ativismo judicial**. Belo Horizonte: Initia Via, 2016, p. 16).

[190] Como no subcapítulo 3.2.

3.1.5.2.1 Projeto de lei "EARN IT Act" (S. 3398 de 2020 e S. 3538 de 2022) e o Início do Combate Legislativo à Criptografia Ponta a Ponta

Inicialmente, explorando a demonstração da produção legislativa nos EUA para regular a aplicação da 4ª emenda, vale enfatizar importante discussão de projeto de lei voltado à responsabilização cível e criminal das pessoas jurídicas que adotam o sistema de criptografia ponta a ponta[191]. É o projeto de lei chamado "EARN IT Act" de 2020 (sigla de *Eliminating Abusive and Rampant Neglect of Interactive Technologies Act*; Projeto de lei S. 3398, na Câmara, e, agora no Senado (2022), sob o número S. 3538)[192], o qual, caso aprovado, pode inviabilizar, ainda que indiretamente, o uso de chaves digitais, como a criptografia ponta a ponta nas comunicações eletrônicas (via WhatsApp, Telegram etc.), por ser imputada conduta ilícita a tais empresas de tecnologia por eventuais omissões na apuração de crimes de pornografia infantil que utilizem suas plataformas digitais como meio material da execução desses delitos. Dadas tais responsabilizações, a doutrina[193] traz críticas a tal projeto legislativo, sob o argumento de violação da 1ª[194] e 4ª emendas da Constituição dos EUA[195], pois contraria a liberdade de expressão (sem a proteção da criptografia há possibilidade de violação de senhas de bilhões de usuários) e demandaria buscas privadas pelas empresas, sem autorização judicial prévia, e, por isso, inconstitucionais – como adiante esmiuçado –, inclusive com repercussões quanto à ilicitude das provas nos processos-crime, desmoralizando a eficácia da justiça penal.

---

[191] UNITED STATES OF AMERICA. House of Representatives. S.3398 – EARN IT Act of 2020. In: UNITED STATES CONGRESS, 116th, 2019-2020, Washington. **Proceedings...** Washington, 2019-2020. Disponível em: https://www.congress.gov/bill/116th-congress/senate-bill/3398/text. Acesso em: 17 out. 2022.

[192] O projeto de lei foi alterado em 2022 no Senado; houve a criação de uma Comissão Nacional de Prevenção à Exploração Sexual Infantil *Online* a fim desenvolver uma cartilha de "Boas Práticas" para orientar e fiscalizar os *providers* a prevenir a exploração infantil e auxiliar na investigação de tais crimes, com a consequente responsabilização, na forma da proposta legislativa.

[193] In: VALLEE, Hannah Quay-de la; AZARMI, Mana. The New EARN IT Act Still Threatens Encryption and Child Exploitation Prosecutions. **Center for Democracy & Technology**, 25 Aug. 2020. Disponível em: https://cdt.org/insights/the-new-earn-it-act-still-threatens-encryption-and-child-exploitation-prosecutions. Acesso em: 15 jun. 2021).

[194] Sobre o tema: REIMAN, Phillip E. Cryptography and the First Amendment: The Right to be Unheard. **Journal of Computer & Information Law**, v. 14, n. 2, p. 325-345, Winter 1996. Disponível em: https://repository.law.uic.edu/cgi/viewcontent.cgi?article=1313&context=jitpl. Acesso em: 18 nov. 2022.

[195] Cf.: NUTHI, Kir. The EARN IT Act Would Give Criminal Defendants a Get-Out-of-Jail-Free Card.Disponível em: https://slate.com/technology/2022/02/earn-it-act-fourth-amendment-violation.html. Acesso em: 20 nov. 2022.

Merece transcrição da crítica que via de regra vem se fazendo sobre o assunto, para a visualização da celeuma nos EUA:

> De fato, pressionar os provedores a conduzir tais buscas parece ser o propósito de levantar a proteção contra responsabilidade do provedor. Essa mudança, na verdade, daria aos fornecedores de CSAM [Child sexual abuse material, ou, material de abuso sexual infantil] um argumento convincente de que a busca do provedor por CSAM é uma **busca inconstitucional sem justificativa conduzida por um agente do governo, cujos frutos devem ser suprimidos**. Além disso, pelo menos **duas leis estaduais impõem responsabilidade criminal aos provedores que não inspecionam o conteúdo compartilhado em suas plataformas em busca de materiais obscenos**. O EARN IT Act removeria o escudo de responsabilidade que os provedores agora desfrutam e **os coagiria a conduzir em nome do governo as buscas sem mandado que a Quarta Emenda proíbe**. Em Illinois, '[uma] pessoa comete obscenidade quando, com conhecimento da natureza ou conteúdo da mesma, ou deixando de exercer uma inspeção razoável que teria revelado a natureza ou conteúdo da mesma", ela "publica ou disponibiliza qualquer coisa obscena'. E na Carolina do Sul, 'Isto é ilegal para qualquer pessoa conscientemente disseminar obscenidade'. Conscientemente é definido como 'ter conhecimento geral do conteúdo do material em questão, ou falhar após uma oportunidade razoável de exercer uma inspeção crível, que teria revelado o caráter do material ou desempenho'. **Esses estatutos obrigariam os provedores a inspecionar o conteúdo de seus usuários e violariam a Quarta Emenda** (Tradução e grifo nossos).

A vantagem da regulamentação por ato legislativo é evitar a necessidade de intervenção judicial a cada nova hipótese surgida de tecnologia, e, avaliar se seu uso para uma busca e apreensão, com base na causa provável, está dentro ou não dos limites da "expectativa razoável de privacidade". Especialmente, frise-se, em casos abrangidos por exceções, como as chamadas "circunstâncias exigentes" na prevenção e rápida repreensão de crimes graves, em atos inclusive ainda não julgados pela Suprema Corte, ou, tecnologias sequer inventadas ou utilizadas para fins de persecução criminal, sabendo-se que a resposta específica a um caso pelo Direito tende a ser atrasada em relação às invenções do homem.

Como visto, a natural alteração do entendimento jurisprudencial acerca da interceptação telefônica veio acompanhada de mudanças legislativas em razão das novas tecnologias, passando a abranger as comunicações eletrônicas. Já em 1986 foi aprovada nos EUA legislação específica para estas comunicações, abrangendo o acesso aos dados armazenados em computador: *The Electronic Communications*

Privacy Act[196] (ECPA). E, seguindo as mudanças tecnológicas no setor de comunicação digital, advieram novas normativas[197]:

> A vigilância eletrônica em tempo real em investigações criminais federais é regida principalmente por dois estatutos": a) a Lei Federal de escutas telefônicas, o Título III do *Omnibus Crime Control* e *Safe Streets Act* de 1968; b) o *Pen Registers* and *Trap and Trace Devices* do Título 18, parte da ECPA.

Dessas novas normas, destaca-se a *USA PATRIOT Act,* que veio para atualizar a ECPA e incluir "comunicações por fio, orais e eletrônicas enquanto essas comunicações estão sendo feitas, estão em trânsito e quando são armazenadas em computadores"[198], aplicando-se ao e-mail, conversas telefônicas e dados armazenados eletronicamente. Todavia, apesar da legislação dos EUA permitir a interceptação telemática em tempo real[199], a criação da E2EE continua obstando a efetividade prática pelas autoridades de persecução penal[200], pelo que há forte movimento para uma redução do alcance da Seção 230[201], visando ao combate aos crimes cibernéticos com alguma responsabilidade aos provedores de internet "ruins".

Calha explicitar, portanto, sobre a chamada Seção 230[202], normativa norte-americana que protege os provedores (mídias digitais) da responsabilidade pela maior

---

[196] Para uma síntese da normativa norte-americana acerca da interceptação telefônica, vide: FERREIRA, Marco Aurélio Gonçalves. A interceptação telefônica em perspectiva comparada (p. 271-289). In: SANTORO, Antonio Eduardo Ramires; MADURO, Flávio Mirza (Org.). Belo Horizonte: D'Plácido, 2017.

[197] Vide: JARRETT, H. Marshall; BAILIE, Michael W. **Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations.** Published by Office of Legal Education - Executive Office for United States Attorneys. 3. ed. 2009. Disponível em: https://www.justice.gov/file/442111/download. Acesso em 19 set. 2022, p. 163.

[198] UNITED STATES OF AMERICA. Department of Justice. Electronic Communications Privacy Act of 1986 (ECPA). Disponível em: https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285. Acesso em 19 set. 2022.

[199] JARRET, *Op. cit*, p. 164.

[200] Deste ponto partem críticas construtivas à atualização da Seção 230, a qual dispõe que "Nenhum provedor ou usuário de um serviço de computador interativo deve ser tratado como o editor ou orador de qualquer informação fornecida por outro provedor de conteúdo de informação" (Tradução nossa). ELECTRONIC FRONTIER FOUNDATION. **Section 230 of the Communications Decency Act**. Disponível em: bit.ly/3UD0OtQ. Acesso em: 19 set. 2022.

[201] UNITED STATES. Department of Justice. **Department of Justice's Review of Section 230 of the Communications Decency ACT of 1996.** Disponível em: https://www.justice.gov/archives/ag/department-justice-s-review-section-230-communications-decency-act-1996. Acesso em 19 set. 2022.

[202] A Seção 230 preconiza, assim, que as mídias digitais, ou, os intermediários *online* que meramente hospedam ou republicam discursos, "são protegidos contra uma série de leis que poderiam ser usadas para responsabilizá-los legalmente pelo que outros dizem e fazem" (LII. **47 U.S. Code § 230**: Protection for private blocking and screening of offensive material. Disponível em: https://www.law.cornell.edu/uscode/text/47/230. Acesso em: 18 out. 2022 – Tradução nossa).

parte do conteúdo gerado pelo usuário (ato de terceiro). Inclusive, o Departamento de Justiça dos EUA

> apoia reformas para deixar claro que a imunidade da Seção 230 não se aplica a um caso específico em que uma plataforma tenha conhecimento real ou aviso de que o conteúdo de terceiros em questão violou a lei criminal federal ou onde a plataforma recebeu uma decisão judicial de que o conteúdo é ilegal em qualquer aspecto. [203] (tradução nossa).

Porém, o *EARN IT Act* pretende alterar a atual disposição legal para permitir demandas cíveis e criminais relacionadas a material relativo ao abuso sexual infantil, justamente, em face de tais plataformas *online*. Logo, esse projeto legislativo torna as proteções da Seção 230 dependentes da prevenção e resposta a esse material ilícito por ato dos provedores, isto é, estes não serão mais protegidos automaticamente, mas exceto se agirem em conformidade com um conjunto de práticas recomendadas para detectar e denunciar materiais de exploração sexual infantil às autoridades, mesmo que não se exclua a E2EE, em lei, expressamente.

Desse modo, é preciso salientar do projeto de lei que a questão da criptografia ponta a ponta não é mencionada diretamente, como determinante de sua quebra, ou a criação de *backdoors* pelas plataformas digitais, mas ela é erigida, expressamente, como uma das "Boas Práticas"[204] criadas para fiscalização por uma Comissão, pressupondo a exigência de alguma brecha na segurança da E2EE, seu enfraquecimento, para fins investigativos criminais[205], e assim, prevenir ou reduzir a exploração sexual infantil.

Veja-se a parte do *EARN IT Act* que é criticado pela doutrina como impositivo tácito de alguma maneira da quebra da criptografia:

> SEC. 3. COMISSÃO NACIONAL DE PREVENÇÃO À EXPLORAÇÃO SEXUAL INFANTIL ONLINE. [...] O objetivo da Comissão é desenvolver as **melhores práticas** recomendadas que os provedores de serviços interativos

---

[203] UNITED STATES. Department of Justice. *Op. cit*.

[204] No mesmo sentido, com base em fala do Senador Blumenthal, defensor do EARN IT: "Não proíbe o uso de criptografia, não cria responsabilidade pelo uso de criptografia, mas **o uso indevido da criptografia para aumentar a atividade ilegal é o que dá origem à responsabilidade aqui**" (Tradução e grifo nossos. Cf.: WILLIE, Matt. EARN IT Act lawmaker finally admits the bill is targeting encryption. **Input**, 13 fev. 2022. Disponível em: bit.ly/3F5onG4. Acesso em: 18 out. 2022).

[205] É "um conjunto de 11 "princípios voluntários" que Facebook, Google, Microsoft, Roblox, Snap e Twitter – prometeram seguir. Embora [...] não afetem especificamente a criptografia o evento teve uma mensagem anticriptografia explícita". Cf.: NEWMAN, Lily Hay. **The EARN IT Act Is a Sneak Attack on Encryption**: The crypto wars are back in full swing. Disponível em: bit.ly/3FwgWcs. Acesso em: 18 out. 2022. (Tradução nossa).

> de computador podem optar por **implementar** para **prevenir**, **reduzir** e responder à exploração sexual *online* de crianças, incluindo aliciamento, tráfico sexual e abuso sexual de crianças e a proliferação de material de abuso sexual infantil *online*. [206] (Tradução e grifo nossos).

Apesar da teórica manutenção da E2EE disposta no projeto legislativo:

> [...] (7) TECNOLOGIAS DE CRIPTOGRAFIA. — "(A) [...] nenhuma das seguintes ações ou circunstâncias servirão como base independente para a responsabilidade de um provedor de um serviço de computador interativo por uma reclamação ou cobrança descrita nesse parágrafo: "(i) O provedor utiliza serviços completos de mensagens criptografadas de ponta a ponta, criptografia de dispositivo ou outros serviços de criptografia. "(ii) **O provedor não possui as informações necessárias para descriptografar uma comunicação.** "(iii) O provedor deixa de tomar uma ação que de outra forma prejudicaria a capacidade do provedor de oferecer serviços completos de mensagens criptografadas de ponta a ponta, criptografia de dispositivo ou outros serviços de criptografia. [...].[207] (Tradução e grifo nossos).

A crítica doutrinária levanta tese perspicaz no caso de aprovação do projeto de lei em comento: a muito provável futura alegação pela Defesa dos acusados de ofensa à 4ª emenda, apesar da intenção legítima da segurança pública com a nova legislação, resultando na exclusão da prova no processo-crime. Tal inconstitucionalidade não adviria por conta de violações de outros direitos e garantias fundamentais do acusado (v.g. a privacidade, o sigilo telefônico), mas porque acabaria com a voluntariedade das plataformas digitais em buscar e denunciar o material ilegal ligado ao abuso sexual infantil por ato de terceiro (*"Good Samaritan" protection*), entregando-o ao conhecido "Centro Nacional para Crianças Desaparecidas e Exploradas". Ora, na forma ora em vigor no ordenamento jurídico norte-americano, tem-se que

> A busca pode ser conceituada como uma atividade de pesquisa, desenvolvida por uma autoridade pública, orientada a um objetivo processual. Engloba todas as possibilidades de pesquisa para a descoberta de provas, como a interceptação eletrônica, a quebra de sigilo, a busca domiciliar, a busca em automóveis, a revista pessoal, a infiltração de agentes secretos em organizações criminosas etc. Um detalhe importante é que **a busca**, no sentido constitucional do termo, **é aquela levada a efeito por um agente público. Toda e qualquer atividade de pesquisa decidida e desenvolvida por um particular não é uma busca no sentido da 4ª emenda; assim decidiu a Suprema Corte em Burdeau v. McDowell, 256 U.S. 465 (1921).** E, por essa razão, não está abrangida pelas limitações da 4ª emenda: não precisa ser razoável**. Contudo, se um particular desenvolve uma pesquisa**

---

[206] CONGRESS.GOV. **S.3538 - EARN IT Act of 2022**. 2022. Disponível em: https://www.congress.gov/bill/117th-congress/senate-bill/3538/text. Acesso em: 18 out. 2022.
[207] *Ibid*.

> **a pedido ou a mando de uma autoridade pública, realiza uma busca**.[208] (Grifo nosso)

Em suma, diante das ameaças de responsabilidades cível e criminal que o *EARN IT Act* pretende imputar às plataformas digitais (setor privado), voltada à determinação proativa da procura de material ilegal, e não apenas relatar algo assim por acaso encontrado (constitucional, portanto), passam a ser encarados como quem faz "as vezes"[209] do Estado; logo, não havendo mandado judicial com os requisitos constitucionais da 4ª emenda obedecidos, tornará a prova ilícita, inservível ao processo-crime.

Diante disso, conclui-se que o debate acirrado que se antevê nas Casas Legislativas e, outrossim, nos tribunais dos EUA, podendo alterar o alcance ou a aplicação das garantias da 4ª emenda, é a decisão sobre a abrangência da cooperação das empresas privadas na investigação criminal de usuários em suas bases de dados, merecendo análise em subcapítulo próprio mais adiante.

Por fim, percebe-se que tal projeto de lei quer se valer da pedofilia e da pornografia infantil como pano de fundo para alavancar sua aprovação legislativa, no que tange à quebra das chaves digitais (criptografia ponta a ponta), dada a impossibilidade cada vez maior de investigação criminal nas mídias digitais, meio que praticamente sucateou a anterior tecnologia telefônica, quando as interceptações não possuíam entraves de segurança pelas empresas privadas de telefonia para a obediência a motivadas ordens judiciais. Essa evidente repetição retórica de zelar pelo interesse das crianças, aliás, como nos vários países a seguir pesquisados, é uma tentativa de obscurecer a intenção de manipular a opinião pública, ainda que socialmente relevante.[210]

3.1.5.2.2 *House Bill* (HB) 57 de 2019[211], do estado de Utah

---

[208] RAMOS, 2006, *op. cit,* p. 118.

[209] BANDEIRA DE MELLO, Celso Antônio. **Curso de Direito Administrativo**. 27. ed. São Paulo: Malheiros, 2010. p. 385.

[210] Neste sentido: RIPOLLÉS, José Luis Díez. **A racionalidade das leis penais**: teoria e prática. Tradução: Luiz Régis Prado. 2. ed. São Paulo: Revista dos Tribunais, 2016, p. 34.

[211] STATE OF UTAH. Electronic Information or Data Privacy. **Legiscan**, H.B. 57, Mar. 2019. Disponível em: https://legiscan.com/UT/text/HB0057/id/1969570. Acesso em: 05 out. 2021.

No plano estadual, vigente nova legislação norte-americana decorrente, coincidentemente ou não, da ideia esposada pelo juiz Alito no caso Jones em hipóteses nela regulamentada. Recentemente promulgada pelo estado de Utah (EUA), a HB 57/2019, chamada de *Electronic Information or Data Privacy Act*, é a primeira lei do país que trata do aludido tema julgado pela Suprema Corte, destacando-se que em outros estados já se verifica igual tendência legislativa, como a Califórnia e Vermont, com legislações dirigidas à proteção da privacidade de dados digitais, mas, por ora, aos direitos do consumidor.[212]

Essa lei, chamada de *Electronic Information or Data Privacy Act*, traz à tona a necessária regulamentação de casos em tese abarcados pelas garantias da 4ª emenda. A lei abrange diversas disposições que tratam da privacidade de informações ou dados eletrônicos, exigindo **que a polícia obtenha um mandado judicial** para a busca em e-mails e as diversas formas de comunicação eletrônica, não só no aparelho (*smartphone*, computador, *tablet* etc.), mas também, no servidor ("nuvem").

Disciplina a HB 57/2019, em suma, que quando os dados ou informações eletrônicas de alguém forem obtidos haja uma notificação ao investigado; e que as **informações eletrônicas e os dados obtidos sem mandado judicial serão excluídos da consideração em processos judiciais.**

Essas "Informações e dados eletrônicos" foram definidos como um sinal, escrita, imagem, som ou inteligência de qualquer natureza transmitida ou armazenada no todo ou em parte por um fio (cabo), rádio, meio eletromagnético, foto eletrônica ou sistema óptico de foto, abrangidas informações de localização, dados armazenados e dados transmitidos de um dispositivo eletrônico.

Nesse sentido, ampliou-se o grau de proteção advindo do caso Carpenter, exigido mandado judicial para uma busca e apreensão pela polícia (garantia da 4ª emenda), "aplicando-o a todos os nossos dados eletrônicos", não só à tecnologia do referido julgado (CSLI), ou, dos dispositivos de uso corpóreo do investigado (celular e microcomputador, por exemplo), mas, inclusive, aos documentos armazenados nos

---

[212] "A Lei de Utah é atualmente a lei mais forte de seu tipo nos Estados Unidos e incentivará outros estados", mas a Lei de Privacidade do Consumidor da Califórnia dispõe apenas a privacidade de dados eletrônicos do consumidor. (Tradução nossa. BOLAMPERTI, Anne; FOWLER, Patrick X. What Does the New Utah Electronic Data Privacy Law Do? **S&W Cybersecurity and Data Security Law Blog**, May 2019. Disponível em: bit.ly/3VGzkF9. Acesso em: 19 nov. 2021).

servidores, como o *Dropbox* ou o *Google Drive*, enquanto, "no passado, a aplicação da lei não tinha a exigência de buscar tais informações por meio de mandado."[213]

Já na primeira disposição da lei se estabelece quando um **mandado emitido por um tribunal por causa provável é necessário**, e, o que, especificamente, **não pode** ser obtido sem um mandado. Além de **exceções** estritas para dispositivos roubados, um mandado de busca será necessário para que a aplicação da lei obtenha informações de localização, dados armazenados ou dados transmitidos de um dispositivo eletrônico para uma investigação ou acusação criminal, bem como informações eletrônicas ou dados enviados pelo proprietário desses dados a um provedor de serviços de computação remota[214], como acima enfatizado.

A lei confere um prazo da intervenção, tal como o art. 5º da nossa Lei de Interceptação Telefônica, de n. 9296/96[215], cabível às interceptações telemáticas[216], inovando quanto à notificação mais imediata que disciplina pela lei brasileira, pois o réu, via de regra, muito posteriormente toma ciência dos atos investigativos. A HB 57/2019 declara que se "informações ou dados eletrônicos" forem obtidos com um mandado, a aplicação da lei deve – no **prazo de 14 dias** após a obtenção das informações específicas no mandado – emitir uma **notificação** ao proprietário das informações que declara, entre outras coisas: "(1) que um mandado foi solicitado e concedido, (2) o tipo de mandado emitido, (3) o período de tempo durante o qual a coleta de informações foi autorizada e (4) o delito especificado no pedido de mandado".[217]

---

[213] CF.: MACDONALD, C. Gov. Herbert signs Bill requiring police obtain search warrants to access electronic information. **Ksl.com**, mar. 2019. disponível em: https://www.ksl.com/article/46520524/gov-herbert-signs-bill-requiring-police-obtain-search-warrants-to-access-electronic-information. Acesso em: 15 nov. 2021.

[214] Como aduzido em BOLAMPERTI; FOWLER, *Op. cit.*

[215] BRASIL. Lei n. 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. **Diário Oficial da União**, Brasília, DF, 25 jul. 1996, p. 13757. http://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 15 nov. 2021: "Art. 5° A decisão será fundamentada, sob pena de nulidade, **indicando também a forma de execução da diligência**, que não poderá exceder **o prazo de quinze dias, renovável por igual tempo** [...]" (grifo nosso).

[216] O STF admite a prorrogação sucessiva do prazo de 15 dias do art. 5º da Lei n. 9296/96 às interceptações telefônicas e às "**comunicações de dados telemáticos**, visto que cláusula tutelar da inviolabilidade **não pode constituir instrumento de salvaguarda de práticas ilícitas.**" (BRASIL. Supremo Tribunal Federal. Habeas Corpus n. 132115/PR. Relator: Ministro Dias Toffoli. Brasília, 06 abr. 2018).

[217] WATZMAN, Alyssa; THOMPSON, Bryan. Utah requires warrant or law enforcement access to certain tuypres of data. **Data Privacy & Cybersecurity**, Apr. 2019. Disponível em: https://lewisbrisbois.com/blog/category/data-privacy-cyber-security/utah-requires-warrant-for-law-enforcement-access-to-certain-types-of-data. Acesso em: 12 out. 2021.

A lei ainda admite exceções, como já indicado no estudo dos julgados da Suprema Corte estado-unidense e pela doutrina[218], quanto às "circunstancias exigentes". Tais exceções da **H.B. 57/2019** são as seguintes, em resumo:

> (2) (a) "Uma agência de aplicação da lei pode obter **informações de localização sem um mandado para um dispositivo eletrônico:** [...] (iv) de acordo com uma **exceção reconhecida judicialmente** para os requisitos do mandado;" [...] (vi) do fornecedor do serviço de computação remota **se o fornecedor do serviço de computação remota revelar voluntariamente a informação de localização**: (A) sob a crença de que existe uma **emergência** envolvendo um **risco iminente de morte**, **ferimentos físicos graves, abuso sexual, exploração sexual em transmissão ao vivo, rapto, ou tráfico de seres humanos**; ou (B) que seja inadvertidamente **descoberta pelo prestador do serviço** de telecomputação e **pareça pertencer ao cometimento de um crime, ou de um delito envolvendo violência física, abuso sexual, ou desonestidade**. (b) Uma agência de aplicação da lei pode obter dados armazenados ou transmitidos a partir de um dispositivo eletrônico, ou informações eletrônicas ou dados transmitidos pelo proprietário da informação eletrônica ou dados a um prestador de serviços de computação à distância, **sem um mandado**: (i) **com o consentimento informado do proprietário do dispositivo** eletrônico ou informações ou dados eletrônico; (ii) de acordo com uma exceção reconhecida judicialmente para os requisitos do mandado; (iii) **em ligação com um relatório enviado pelo Centro Nacional para Crianças Desaparecidas e Exploradas com menos de 18 anos de idade** [...]. (Tradução e grifo nosso).

Observa-se que a legislação estadual acabou por vir ao encontro da doutrina e jurisprudência da Suprema Corte dos EUA, no intuito da criação de uma norma geral e abstrata que, previamente, trará um norte ao bom funcionamento da polícia quanto às (im)possibilidades nas investigações criminais, e, por conseguinte, ao devido processo legal no eventual processo-crime decorrente, quanto às garantias da 4ª emenda, sobretudo.

---

[218] Nos termos delineados no rodapé n. 156.

3.1.5.2.3 Projetos de Lei H.R.[219] 7891[220] e S. 4051[221], referentes à Lei de Acesso Legal a Dados Criptografados (*Lawful Access to Encrypted Data Act*)

Trata-se de recente produção por lei[222] sobre a criptografia digital nos meios de comunicação. Determina tal inovação legislativa que as empresas de tecnologia, as quais a ela se subsuma, garantam a possibilidade de descriptografar ou decodificar informações sob a E2EE em seus serviços e produtos para fornecimento às autoridades responsáveis pela persecução penal, mediante prévio mandado de busca e apreensão do juízo competente, sob a 4ª emenda.

Exige-se, outrossim, preencher o requisito da individualização do próprio dispositivo objeto da ordem judicial, ou seja, não pode ser genérico, e mais, as informações buscadas, e eventualmente obtidas, devem ser isoladas pelo agente, justo em razão da abrangência de informações que um *smartphone* pode trazer nos dias atuais, evitando-se abuso ou excesso na investigação e na intromissão ao direito à privacidade do cidadão.

Por isso, correta a tese na doutrina brasileira da necessidade da existência de lei às intervenções processuais penais nos aparelhos de telefonia multifuncional (*smartphones*), nos casos previstos pelo ordenamento jurídico, aliada à exigência de as medidas judiciais cautelares sejam as mais detalhadas possíveis (ainda que, eventualmente, sob novo pedido após constatado pela perícia policial a existência de aplicativos diversos do pleiteado na exordial pelo Ministério Público ou pela autoridade policial):

---

[219] Originário o projeto de lei da Câmara dos Representantes dos Estados Unidos (*House of Representatives*), daí o termo "H.R." (UNITED STATES OF AMERICA. House of Representatives. **Bills & Resolutions**. Disponível em: https://www.house.gov/the-house-explained/the-legislative-process/bills-resolutions. Acesso em: 28 nov. 2021).

[220] Vide: UNITED STATES OF AMERICA. House of Representatives. H.R.7891 – Lawful Access to Encrypted Data Act. In: UNITED STATES CONGRESS, 116th, 2019-2020, Washington. **Proceedings...** Washington, 2019-2020. Disponível em: https://www.congress.gov/bill/116th-congress/house-bill/7891/text#toc-H8D2533E6D74E44A2AC049571DCA1C454. Acesso em: 17 out. 2022.

[221] Cf.: UNITED STATES OF AMERICA. Senate. S.4051. Lawful Access to Encrypted Data Act. In: UNITED STATES CONGRESS, 116th, 2019-2020, Washington. **Proceedings...** Washington, 2019-2020. Disponível em: https://www.congress.gov/bill/116th-congress/senate-bill/4051/text. Acesso em: 17 out. 2022. Projeto de lei relacionado ao texto da Câmara (H.R. 7891): "*Related Bills*".

[222] Proposta bicameral iniciada em 2020: na Câmara H.R. 7891, no Senado S. 4051. Da análise do andamento nas casas legislativas nos endereços eletrônicos supra (17 out. 2022), ambos os projetos de lei foram agora encaminhados à Comissão do Poder Judiciário, além das Comissões de Inteligência (*Permanent Select*), Ciência, Espaço e Tecnologia.

> **O acesso aos distintos aplicativos reclama autorizações judiciais precisas:** acesso a mensagens trocadas pelo WhatsApp, acesso a dados bancários, acesso a contas de *e-mail*, tudo isso **reclama da autoridade judicial que examine as distintas formas de afastamento da privacidade.** Assim, a rigor, **para que a polícia examine dados bancários, telefônicos, contas de *e-mail*, o aplicativo WhatsApp, tudo deve ser detalhadamente requerido e examinado pelo juízo, sob pena de se estabelecer indevidas quebras não autorizadas a sigilos protegidos pela lei e pela Constituição da República.** Aliás, o acesso ao telefone celular, mediante uma autorização genérica, poderia consistir em um "atalho" que facilitaria, mediante apenas um pedido e uma decisão, acesso a múltiplas dimensões da privacidade, considerando que o aparelho celular, como já referido, é, ao mesmo tempo, um facilitador e um mecanismo de armazenamento de informações.[223] (Grifo nosso).

A responsabilidade abrange fabricantes de dispositivos (celulares) e sistemas com informações no próprio aparelho, ou, com informações guardadas de forma remota (nas nuvens).

Estabelece o projeto legislativo os requisitos e procedimentos para auxiliar as agências de aplicação da lei no acesso a dados criptografados, apontando o Congresso, como justificativa da nova legislação proposta, verdadeiro resumo de parte de toda a situação já reportada nesta dissertação, principalmente o fato de a criptografia nos meios digitais ser um espaço no qual criminosos atuam quase que sem qualquer possibilidade, mesmo mediante autorização judicial e sob os fundamentos da 4ª emenda da Constituição dos EUA, da devida investigação criminal, com uma apontada desídia (ao que tudo indica proposital) das empresas responsáveis ao não desenvolverem a tecnologia apropriada para alterar essa situação.

Dos aludidos fundamentos do legislador, na H.R. 7891, enfatizem-se os seguintes pontos[224]:

> (1) O **uso crescente de criptografia à prova de mandado em dispositivos, plataformas e sistemas diários permite que atores ilegais envolvidos em atividades criminosas perigosas** – incluindo abuso sexual infantil, terrorismo e tráfico internacional de drogas – **usem criptografia para proteger suas atividades ilícitas de autoridades**. (2) **Por causa da criptografia à prova de mandado, o governo muitas vezes não consegue obter as evidências eletrônicas e inteligência necessárias para investigar e processar ameaças à segurança pública e nacional, mesmo**

---

[223] GLOECKNER, Ricardo Jacobsen; EILBERG, Daniela Dora. Busca e apreensão de dados em telefones celulares: novos desafios diante dos avanços tecnológicos. **Revista Brasileira de Ciências Criminais**, São Paulo, v. 156, p. 353-393, jun. 2019, p. 5.

[224] In: UNITED STATES OF AMERICA. House of Representatives. H.R.7891 – Lawful Access to Encrypted Data Act. In: UNITED STATES CONGRESS, 116th, 2019-2020, Washington. **Proceedings...** Washington, 2019-2020. Disponível em: https://www.congress.gov/bill/116th-congress/house-bill/7891/text#toc-H8D2533E6D74E44A2AC049571DCA1C454. Acesso em: 17 out. 2022.

> **com um mandado ou ordem judicial.** Isso fornece um **'espaço sem lei'** que criminosos, terroristas e outros atores mal-intencionados podem explorar para seus fins nefastos. **(3) Muitos provedores de serviços, fabricantes de dispositivos e desenvolvedores de aplicativos que usam criptografia não implementam a tecnologia que permitiria ao governo obter as evidências eletrônicas necessárias para investigar e processar ameaças à segurança pública e nacional**. (4) **A Quarta Emenda à Constituição dos Estados Unidos estabelece um equilíbrio entre a expectativa razoável de privacidade do cidadão individual por um lado e, por outro, a necessidade legítima de o governo obter acesso aos espaços mais íntimos dos cidadãos.** Vive para proteger o público de atores criminosos. (5) **Os autores da Constituição forneceram barreiras específicas para a intrusão do governo no espaço privado e íntimo do indivíduo** – ou seja, que o governo deve mostrar por causa provável que a evidência de um crime existe naquele espaço íntimo e deve ter um magistrado neutro, desvinculado do interesse da aplicação da lei, aprovar o pedido da aplicação da lei e emitir um mandado. **(6) Uma vez que o governo satisfaça o ônus de mostrar a causa provável a um magistrado neutro, o governo tem o direito de pesquisar e apreender evidências de um crime no espaço privado de um indivíduo**. (7) Esse **equilíbrio cuidadoso de interesses estabelecido pelos Fundadores continuou a ser calibrado ao longo da história dos Estados Unidos à medida que surgiam diferentes desafios, incluindo, mais notavelmente, os avanços tecnológicos na vida diária**. Por exemplo, o Congresso impôs requisitos legais adicionais que o governo deve cumprir e que um juiz deve considerar satisfeitos antes que um tribunal possa autorizar a interceptação de comunicações. **Mas o direito do indivíduo à privacidade nunca foi absoluto. (8) Se não for abordado, o anonimato criminal acionado pela tecnologia de criptografia de ponta a ponta continuará a representar um sério risco para o público**. (9) No entanto, os avanços na tecnologia continuam sem a devida consideração das questões de acesso legal. (10) Além disso, **muito poucos, ou nenhum, recursos do setor privado ou de instituições de ensino e pesquisa são dedicados à busca de soluções tecnológicas para fornecer acesso legal em diferentes plataformas tecnológicas criptografadas**. **(11)** Mais recursos devem ser dedicados para incentivar as melhores mentes nos Estados Unidos a pesquisar as questões descritas nesta seção e decidir **como fornecer os produtos e serviços mais seguros aos clientes, ao mesmo tempo que fornece acesso às autoridades policiais às informações de que o governo precisa para investigar criminosos que procuram causar danos ao público e proteger a segurança nacional**. (Tradução e grifo nossos).

Da análise desse projeto de lei de versão número 7891, destacam-se de seus dispositivos que deve haver, em regra, ordem de um juízo competente, através de mandado de busca e apreensão com base na causa provável, que autoriza a busca de um dispositivo eletrônico ou informações eletrônicas armazenadas remotamente; e, uma vez recebida esta moção, o juízo do local competente, "em apoio" (como no caso de cartas precatórias no Brasil), aliado a fundamentos razoáveis para acreditar que a assistência exigida pelo pedido ajudará na execução do mandado, cabível solicitar que um fabricante de dispositivo, um provedor de sistema operacional, um provedor de serviço de computação remota ou outra pessoa, forneça todas as informações, instalações e assistência necessária para acessar informações

armazenadas em um dispositivo eletrônico ou para acessar informações eletrônicas armazenadas remotamente, conforme autorizado pelo mandado de busca e apreensão.

Importante notar da regra legal proposta que as informações, instalações e assistência solicitadas a serem fornecidas nos termos acima **devem incluir o fato de se procurar isolar as informações autorizadas a serem pesquisadas** (evitando-se a busca genérica diante do grau de informações exacerbado que contem em *smartphones*, por ex.), **descriptografar ou decodificar** informações no dispositivo eletrônico ou informações eletrônicas armazenadas remotamente objeto do mandado judicial, ou ainda, demonstrando o rol aberto para a efetividade da medida, de outra forma fornecer tais informações em um formato inteligível; por fim, pode conter na ordem judicial a determinação de **se fornecer suporte técnico conforme necessário para garantir a execução eficaz do mandado para os dispositivos eletrônicos particularmente nele descritos**.

Esse projeto, caso aprovado, certamente revolucionará o resto do mundo, pois, reitere-se, as principais empresas de mensageria são sediadas nos EUA. Mas não só por isso, a repercussão se estenderá a outros países, porque os fundamentos constitucionais do projeto legislativo, apesar de toda a discussão sobre a possibilidade técnica da descriptografia ou decodificação, em seus estritos termos e de análise no plano abstrato, não fere o devido processo legal[225], pelo contrário, está de acordo com os direitos e garantias processuais penais já pacificados não somente no direito norte-americano, mas também, no brasileiro, como a individualização dos mandados de busca e apreensão (vedação a mandados genéricos) e a interceptação telemática mediante prévia decisão judicial.

Tem-se ciência que muitos migrarão a outros aplicativos de mensagens dotados de criptografia ponta a ponta, não sediados em solo norte-americano, como o Telegram. Entretanto, pelos bilhões de usuários dos aplicativos de origem norte-americanos (como o WhatsApp e o Facebook Messenger) e a possibilidade de decodificação de aparelhos celulares que também trocarão mensagens com esses que se utilizam de serviços estrangeiros, já trará efeitos imediatos à investigação criminal. Note-se: os próprios fabricantes de aparelho celular podem programar os *smartphones* a não aceitarem o *download* de aplicativos fora de um rol permitido em

---

[225] Nesse sentido: RAMOS, João Gualberto Garcez. **O Devido Processo Legal no Contexto do Processo Penal Adversarial e sua Evolução na Suprema Corte dos EUA.** Goiânia: Lutz, 2022.

sua loja virtual, como o Google Play (sistema operacional Android) e a App Store (loja oficial de aplicativos para o sistema operacional iOS e iPadOS da Apple). E isso pode se operar a bilhões por todo o planeta, uma excelente ferramenta para tentar obstaculizar o uso de aplicativos fora do rol da legislação, de empresas estabelecidas formalmente, já que a chance de criação de celulares e aplicativos voltados à criminalidade é uma realidade.

O que se conclui desta geral demonstração do que há em debate nos Estados Unidos é o objetivo desta quebra das chaves digitais (E2EE), utilizando-se de tema sensível e midiático (pedofilia e pornografia infantil) para influenciar sua aprovação legislativa diante da dificuldade de investigação criminal nas mídias digitais.

Interessante é o exemplo da prática forense em relação ao dispositivo Alexa, da Amazon. Seus advogados levantaram tese jurídica para negar o cumprimento à requisição do Ministério Público de acesso aos dados guardados em nuvem, sob os argumentos de violação das 1ª e 4ª emendas; todavia, o caso não chegou a ser julgado por divulgação de espontânea vontade do conteúdo pelo usuário[226]:

> No entanto, há um problema adicional com dispositivos como o Alexa. Um dispositivo que está sempre ouvindo uma palavra de comando e, em seguida, começa uma gravação de som sempre que a palavra de comando é fornecida, **potencialmente permite muitas invasões em uma pessoa em sua própria casa. Dispositivos eletrônicos "inteligentes" modernos contêm uma infinidade de dados que podem "revelar muito mais em combinação do que qualquer registro isolado", permitindo que aqueles com acesso a eles reconstruam "[a] soma da vida privada de um indivíduo". Riley v. Califórnia**, 134 S. Ct. 2473, 2489 (U.S.S.C. 2014). A Amazon argumenta que a proteção da Primeira Emenda deve ser estendida não apenas às pesquisas e respostas de Alexa, mas também às gravações e transcrições reais do que o usuário está ordenando que Alexa faça. (Tradução nossa).

Com esse exemplo é demonstrado, novamente, um debate acirrado que se antevê pela frente a se resolver pelo Poder Judiciário: até que ponto irá a cooperação das empresas privadas na investigação criminal pelos dados de usuários em suas bases de dados.

---

[226] Extraído de: FISHER, Alexis. First Amendment Issues with the Amazon Alexa. **Ristenpart Law**. Disponível em: https://www.ristenpartlaw.com/news-and-updates/first-amendment-issues-with-the-amazon-alexa. Acesso em: 5 jun. 2021.

3.2 O REINO UNIDO E A E2EE: UMA NOVIDADE TECNOLÓGICA NO PROJETO DE LEI *ONLINE SAFETY BILL*

No Reino Unido, o projeto de lei conhecido como *Online Safety Bill* pretende estabelecer uma nova estrutura regulatória para lidar com conteúdo nocivo na internet, impondo um dever legal de cuidado a certos provedores de serviços no meio digital para moderar o conteúdo gerado pelo usuário, a fim de que os demais não sejam expostos a tais ilegalidades, com previsão de multas e penalidades para as pessoas físicas e jurídicas que não cumprirem esse dever, inclusive de natureza criminal[227].

De acordo com o "dever de cuidado" (*duty of care*) disposto no projeto de lei (Seção 117), as empresas de tecnologia que hospedam conteúdo gerado pelo usuário ou permitem que as pessoas se comuniquem serão legalmente obrigadas a identificar, remover e limitar proativamente[228] a disseminação de conteúdo ilegal e legal, mas prejudicial – como abuso sexual infantil, terrorismo e material suicida – ou podem ser multados em até 10% de seu faturamento pelo regulador de danos online, o *Ofcom* (abreviação de *Office of Communications*), agência reguladora de mídia do Reino Unido e prevista no referido projeto de lei como órgão fiscalizador do conteúdo disseminado na internet por tais provedores ou plataformas digitais.

Porém, para cumprir esse requisito e seu "dever de cuidado", os provedores de serviços, provavelmente, precisarão recorrer a filtros de *upload* e outros mecanismos que possam interferir no uso da criptografia de ponta a ponta. Por conta disso, a novidade nesse projeto é a criação de instrumento tecnológico que promete manter a E2EE através do *software* denominado CSS (do inglês *client side scanning*, traduzido como: "varredura do lado do cliente")[229], mas que já é alvo de debates por sua alegada (in)compatibilidade técnica com a manutenção do sigilo pela criptografia, abrindo brechas para intrusão de terceiros maliciosos.

---

[227] O projeto de lei do Reino Unido pode levar CEOs de tecnologia à prisão, pois prevê (com *vacatio legis* de 2 meses após vigente) a responsabilidade criminal contra executivos que "não cooperem com solicitações de informações do regulador" (Tradução nossa. Cf.: LOMAS, Natasha. Tech CEOs to face faster criminal liability under UK online safety law. Disponível em: https://techcrunch.com/2022/03/16/online-safety-bill-parliament/. Acesso em 17 out. 2022).

[228] Lembrando da tese de se ferir a 4ª emenda nesta hipótese, cf. rodapé n. 208.

[229] Haverá o *download* do *software* CSS em "*smartphones*, *tablets* e computadores para realizar a varredura algorítmica de texto, imagens, vídeos e arquivos para conteúdo proibido antes de ser enviado pelo dispositivo", impedindo que seja remetido e pode alertar a polícia (HAYES, Julian. Online safety: the encryption dilemma - trade-offs. **United Kingdom**, August 18 2022. Disponível em: bit.ly/3h1DLLC. Acesso em 14 out. 2022, Tradução nossa).

De qualquer maneira, através do *Online Safety Bill*, que há anos tramita no Reino Unido, a CSS é uma promessa do Legislativo na tentativa de solucionar todo este imbróglio técnico. Mas, como dito, os especialistas divergem sobre a proposta:

> Os proponentes do CSS o aclamam como uma solução tecnológica minimamente intrusiva que protege o público, evita as preocupações tradicionais de segurança sobre backdoors secretos em comunicações criptografadas por meio de 'protocolos fantasmas ou 'chaves de garantia', deixa o E2EE intacto e reconcilia as demandas concorrentes de aplicação da lei e privacidade ativistas. Os opositores do CSS argumentam que ele constitui uma forma insidiosa de vigilância em massa [...]; que é propenso a erros e manipulação por criminosos sofisticados/Estados hostis; e que é passível de "*scope creep*" – uma vez aceito em princípio, a tentação de procurar outras ofensas e comportamentos socialmente censuráveis se tornará irresistível. [230] (Tradução nossa).

Em síntese, alguns aduzem que a CSS, na realidade, fragiliza a segurança tecnológica da E2EE[231] por atos de terceiros de má-fé[232] e cria sistemática de fiscalização exacerbada e indiscriminada da vida privada ("em massa"), ainda que não planejada inicialmente como um dos objetivos e limites da nova legislação (criticado por ser *scope creep,* traduzido: oportunista); e, há ainda a indicação da tese de suficiência do fornecimento de metadados[233] pelos provedores desses serviços.

De outro lado, os defensores da nova legislação proposta prometem que seria mantida a E2EE, aduzindo ser um método menos intrusivo que a criação de *backdoors* ou o uso de outras técnicas de informática na investigação criminal[234], já que estes

---

[230] *Ibid*.

[231] O governo poderia resolver o problema "de forma mais eficaz expandindo o alcance do projeto de lei para incluir comunicações privadas, mas isso constituiria [violação] de direitos individuais e exigiria que os serviços quebrassem a criptografia" (p. 6, tradução nossa – TRENGOVE, Markus et al. A critical review of the Online Safety Bill. **Patterns**, v. 3, n. 8, Aug. 2022. DOI: https://doi.org/10.1016/j.patter.2022.100544. Acesso em: 17 out. 2022.

[232] "Não há backdoor de criptografia viável que também não possa ser usado por agentes mal-intencionados. [...] "backdoor de criptografia segura" é um oxímoro" (WILTON, Robin. Encryption myths versus realities of Online Safety Bill - The UK government can't legislate the impossible – a safer society depends on encryption, not breaking it. Disponível em: bit.ly/3uwq6zw. Acesso em: 15 out. 2022).

[233] "[...] a análise de metadados pode apenas sugerir atividades ilegais em potencial e provavelmente seria insuficiente para a aplicação da lei obter um mandado de busca para investigação adicional. Da mesma forma, os serviços de 'age-gating' são passíveis de subversão – as pessoas mentem sobre sua idade." (HAYES, *Op. cit*, Tradução nossa).

[234] "[...] ela estabelece claramente, pela primeira vez, os poderes de vigilância de que dispõem os serviços de inteligência e a polícia." (tradução e grifo nossos). In: MACASKILL, Ewen. 'Extreme surveillance' becomes UK law with barely a whimper. **The Guardian**, 19 nov. 2016. Disponível em: https://www.theguardian.com/world/2016/nov/19/extreme-surveillance-becomes-uk-law-with-barely-a-whimper . Acesso em: 20 dez. 2021.

sim implicariam em verdadeira quebra da criptografia (no mínimo a facilitação disso por terceiros maliciosos).

Permanece, todavia, ausente efetiva comprovação da promessa da novidade tecnológica da CSS, repetindo-se constatação do exame das propostas legislativas norte-americanas: a única maneira de os provedores de serviços que oferecem criptografia de ponta a ponta cumprirem esse dever de cuidado seria remover ou enfraquecer a criptografia que eles oferecem.

Inobstante a pretensa lei não proíba a E2EE de forma direta[235], as responsabilidades que ela impõe aos provedores de serviços o fazem implicitamente, tal como o projeto de lei norte-americano *EARN IT Act*. Em tese, inviolável por terceiros de fora da conversa dotada de E2EE, a ausência de criptografia, ou sua fragilização, permitiria que os provedores de serviços interceptassem as comunicações dos usuários para evitar a violação do dever de cuidado imposto a eles.

Enfim, o caso demanda estudo por perícia imparcial a eventual juízo de valor legislativo ou judicial, pois, caso verdadeira, a implantação por lei da CSS é uma novidade que ajudaria a reduzir a polêmica de ofensa à privacidade de forma irrecuperável em face da segurança pública, mantendo-se a criptografia ponta a ponta, relevante não só do ponto de vista dos serviços de mensageria digital, mas de transações econômicas, envio de informações sigilosas empresariais e da vida privada dentro desses aplicativos, dentre outras.

3.3 ALEMANHA: ESTRATÉGIA LEGAL DIFERENCIADA À INVESTIGAÇÃO DE MENSAGENS CRIPTOGRAFADAS PONTA A PONTA

Denota-se que o avanço tecnológico vem modificando o anseio social alemão por novas respostas legislativas, tal como constatado pela Suprema Corte e doutrina norte-americana. Tanto que, a respeito do artigo do Código de Processo Penal da Alemanha, o qual trata de interceptações telefônicas (§100a StPO), a doutrina[236]

---

[235] VOGE, Callum; WILTON, Robin. Internet Impact Brief End-to-end Encryption under the UK's draft Online Safety Bill. **Internet Society**, 5 Jan. 2022. Disponível em: https://www.internetsociety.org/resources/doc/2022/iib-encryption-uk-online-safety-bill/. Acesso em: 14 out. 2022.

[236] Sobre o tema: GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. **O direito de proteção de dados no processo penal e na segurança pública**. Rio de Janeiro: Marcial Pons, 2021, p. 121.

indica 40 alterações legislativas desde 1968, com a mais recente a ora objeto desta dissertação, diante da necessidade de medida legal excepcional de infiltração *on line* de métodos de telecomunicação dotados de criptografia.

Nesta seara, adveio a "*Gesetz zur effektiveren und praxistauglicheren Augestaltung des Strafverfahrens*" (Lei sobre a Organização mais eficaz e viável do Processo Penal)[237], a mais recente legislação federal (2017) e que alterou o capítulo do Código de Processo Penal da Alemanha. Trata da interceptação telemática, criticada desde sua tramitação legislativa pelos argumentos de violação constitucional[238] (v.g. direito à privacidade, com abertura demasiada para interpretações sobre sua aplicabilidade), pois almeja monitorar comunicações através de serviços de mensagens protegidos pela criptografia ponta a ponta mediante a instalação, pelas autoridades legitimadas (Estado), de *software* (*Staatstrojaner*) que se aninha secretamente no dispositivo celular e passa os dados a seus operadores, em crimes específicos mas de extenso rol, como homicídio, roubo, fraude via *web*, evasão fiscal, terrorismo, dentre outros, definidos nessa lei.

A interceptação de fluxo pelo Estado alemão é diferenciada dos demais projetos legislativos examinados até aqui e, por isso, merece destaque. Ele ocorre antes da criptografia ou depois da descriptografia (na tela dos interlocutores; "*source TKÜ*"), mediante a exploração das falhas de segurança no *software*. É o chamado *hacking* do Estado, ou cavalo de Troia do Estado.

Com isso, referida lei alemã promete manter a criptografia ponta a ponta[239]. Não há a obrigação de abertura de tais chaves ao Estado alemão, trazendo essa solução tecnológica, o que, em tese, evitaria discussões jurídicas infindáveis em jogo divergente de juízo de valor quanto à ponderação de princípios constitucionais (segurança pública *versus* privacidade, em síntese) ou, talvez, intransponíveis sob o

---

[237] DEUTSCHLAND. Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens. **Bundesgesetzblatt Teil I**, Bonn, n. 58, ago. 2017. Disponível em: bit.ly/3B9andl. Acesso em: 9 set. 2021.

[238] DEUTSCHER BUNDESTAG. **Pro und Contra Staats-trojaner bei der Anhörung zur Strafrechts-reform**. Berlin, 2017. Disponível em: https://www.bundestag.de/dokumente/textarchiv/2017/kw22-pa-recht-strafrecht/508168. Acesso em: 10 set. 2021.

[239] Deve "haver *backdoors* na criptografia dos serviços de mensageiro? Não, não se fala disso na Alemanha. [...] disse o ministro do Interior, Thomas de Maizière" (tradução nossa). In: SOKOLOV, Andrej. Was die Überwachung der Messenger bedeutet. **WirtschaftsWoche**, Düsseldorf, jun. 2017. Disponível em: https://www.wiwo.de/technologie/digitale-welt/whatsapp-was-die-ueberwachung-der-messenger-bedeutet/19972834.html. Acesso em: 10 set. 2020.

ponto de vista do direito internacional, em razão das sedes das empresas em diversos países[240].

A informação prática a respeito da E2EE é de que já desenvolvida tecnologia à Alemanha para a interceptação telemática pela polícia, independentemente da cooperação ou obrigação das empresas de tecnologia do fornecimento de chaves ou quebra da criptografia:

> Apenas os fornecedores de Internet são afetados pela lei ora aprovada, em particular (mas não apenas) 'através do apoio ao desvio das telecomunicações' às respectivas autoridades. [...] **a abolição da criptografia não é explicitamente uma das obrigações da empresa** [...].[241] (tradução e grifo nossos).

É preciso realçar que na Alemanha, segundo entendimento jurisprudencial, através da ideia de preservação da "capacidade de funcionamento da justiça penal" o processo-crime é voltado a um fluxo investigativo sob o escopo do lema, incisivo, de que o crime não reste impune, como um "dever de se realizar a justiça", obedecidos os direitos fundamentais da privacidade e do sigilo das comunicações:

> O limite a que a jurisprudência recorre com maior frequência no âmbito do processo penal é a chamada ***capacidade de funcionamento da justiça penal*** (*Funktionstüchtigkeit der Strafrechtspflege*). A ideia é **derivada do próprio princípio do Estado de Direito**, que se extrai da Lei Fundamental por via de uma leitura conjunta dos arts. 1 III, 20 III, 28 I GG. **Esse princípio imporia não apenas como uma barreira à persecução penal, como também um dever de realizar a justiça e, portanto, de cuidar para que o crime não permaneça impune.** [...] Os métodos de investigação têm de ser concebidos a partir do direito fundamental ao sigilo das comunicações (*Fernmeldegeheimnis*) e da privacidade da pessoa humana; eles têm de ser limitados por instrumentos processuais de proteção ou por direitos de participação. No que diz respeito ao dever de suportar uma interceptação telefônica, chegou-se, ao que parece, a um resultado satisfatório.[242] (Grifo nosso).

Tal linha de atuação alemã, portanto, num primeiro momento, pode evitar futuro embate judicial com as *Big Techs* acerca da cooperação investigativa para

---

[240] Daí a relevância da Convenção de Budapeste, tratada em tópico específico desta dissertação.

[241] In: BEUTH, Patrick. Bundestag genehmigt Staatstrojaner für alle. Die Bundespolizei sowie alle 19 Nachrichtendienste in Deutschland dürfen künftig Computer und Smartphones von Verdächtigen hacken. Die wichtigsten Bestandteile der neuen Regelungen – und erste Reaktionen. **Spiegel Netzwelt**, 10 Juni 2021. Disponível em: bit.ly/3Hh2uqc. Acesso em: 20 out. 2022.

[242] In: WOLTER, J. **O inviolável e o intocável no direito processual penal**: reflexões sobre dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal. Organização, introdução e tradução: Luís Greco; tradução: Alaor Leite e Eduardo Viana. São Paulo: Marcial Pons, 2018; p. 49 e 202.

angariar provas digitais, como se anuncia nos Estados Unidos, algo extremamente penoso às vítimas e à efetividade da justiça penal, de um lado, e o risco a direitos ligados à privacidade, de outro.

Ocorre que já havia crítica de parte dos partidos políticos contrários quando em votação dessa lei no Parlamento alemão, com reclamações várias pendentes de julgamento na Suprema Corte germânica[243], como o argumento de que a lei que alterou o CPP alemão é muito invasiva à privacidade e não se ter controle judicial sobre eventuais vazamentos dessa tecnologia, já que o método de criação de *software* de espionagem pode ensejar seu uso ilícito por terceiros mal intencionados, como no caso *WannaCry*[244].

A doutrina aponta três pontos principais objeto de reclamação constitucional em face da nova legislação alemã que trata da infiltração *on line*: **a)** "em razão da amplitude do catálogo de fatos" (o BVerfG já estabeleceu que só seria justificável em razão de perigos concretos para bens jurídicos extremamente importantes, mas na lei há crimes de menor relevância, como a falsificação de moeda, a lavagem de dinheiro, a corrupção e a receptação); **b)** "proteção ineficiente do núcleo da esfera privada", pois a norma não prevê uma proibição absoluta de levantamento de dados sem relação com o crime investigado, bem como, não teria fixado juízo de valor pelo magistrado acerca do acesso a tais informações puramente privadas antes do acesso aos órgãos de persecução penal; **c)** a "desproporcional ausência de norma que garanta a mesma proteção dos profissionais dispensados do testemunho aos seus auxiliares, de forma que não se possa, por via transversa – acessando, por exemplo, os dispositivos informáticos da secretária do advogado –, esvaziar as garantias do sigilo profissional".[245]

---

[243] Em consulta no *site* da Suprema Corte Alemã, e, confirmado por email ao setor competente com resposta em 28 out. 2022, tais reclamações constitucionais (BvR 897/18, BvR 1797/18, BvR 1838/18, BvR 1850/18, BvR 2061/18) ainda não foram julgadas (Disponível em: https://www.bundesverfassungsgericht.de/EN/Verfahren/Jahresvorausschau/vs_2022/vorausschau_2022.html. Acesso em: 21 out. 2022).

[244] É o "ransomware que colocou boa parte do mundo (incluindo o Brasil) em um caos enorme, paralisando grandes órgãos [MPSP, o TJSP, o INSS] um *malware* que 'sequestra' arquivos das máquinas ao criptografá-los, e, posteriormente, pedem dinheiro para [os] devolver" (Vide: MUNHOZ, Vinicius. WannaCry, o ransomware que fez o mundo chorar na sexta-feira (12). **Tecmundo**, maio 2017. Disponível em: https://www.tecmundo.com.br/malware/116652-wannacry-ransomware-o-mundo-chorar-sexta-feira-12.htm. Acesso em: 10 set. 2021).

[245] Cf.: GRECO, Luís; GLEIZER, Orlandino. A infiltração online no processo penal: notícia sobre a experiência alemã. **Revista Brasileira de Direito Processual Penal**, Porto Alegre, v. 5, n. 3, p. 1483-1518, set./dez. 2019; p. 28-29. Disponível em: http://www.ibraspp.com.br/revista/index.php/RBDPP/article/view/278. Acesso em: 20 nov. 2021.

Outrossim, o estudo da lei alemã exige cautela para a visão do jurista brasileiro, tendo em vista a influência do Direito Administrativo Sancionador e das interpretações jurisprudenciais e doutrinárias peculiares do direito processual penal interno[246]. Da análise histórica do direito à prova no direito alemão, por exemplo, calcada em julgamentos da sua Suprema Corte, tem-se como corolário o fato de as partes terem

> um direito constitucionalmente garantido de ver produzidas no processo as provas indicadas e propostas que representam uma efetiva relevância ou utilidade para a resolução da controvérsia; a este direito corresponde à obrigação do juiz de introduzir tais meios de prova, sob pena de violação do preceito do art. 103, § 1º[247], do *Gundgesetz*.[248]

Não seria, assim, um mero interesse das partes em ver a prova produzida, vinculando-se ao poder discricionário decisivo do juiz sobre a sua relevância: fixou-se na Alemanha o princípio de que, quando pertinente, deve o magistrado determinar a produção da prova requerida, obviamente, afastadas as produções probatórias proibidas pela sua Constituição e Código de Processo Penal[249].

Há também várias reclamações constitucionais em andamento contra o uso de *Trojans* estaduais, previstas agora também nas leis de seus estados, como de Baden-Württemberg e Hamburgo (dentre outras já julgadas[250]), mas tidas como inadmissíveis pelo Tribunal Constitucional Federal da Alemanha, por questões formais: os reclamantes não explicaram por qual motivo não se ajuizou ação declaratória ou medida cautelar perante o tribunal administrativo, ferindo regra de subsidiariedade, e, os regulamentos impugnados não contiveram especificações sobre a natureza, funcionalidade e controle de aplicação do software de vigilância,

---

[246] Cf.: BUSATO, Paulo César. Razões político-criminais para a responsabilidade penal das pessoas jurídicas. In: BUSATO, Paulo César; GRECO, Luís (Coord.). **Responsabilidade penal de pessoas jurídicas**: seminário Brasil-Alemanha. Florianópolis: Tirant Lo Blanch, 2018, p. 59).

[247] DEUTSCHLAND. Deutscher Bundestag. Grundgesetz für die Bundesrepublik Deutschland. Disponível em: bit.ly/3Yeg6IT. Acesso em: 13 set. 2022. Destaque-se: "*Artikel 103 (1) Vor Gericht hat jedermann Anspruch auf rechtliches Gehör.*" (Tradução: "Artigo 103 (1) Todos têm direito a ser ouvidos no tribunal").

[248] AVOLIO, Luiz Francisco Torquato. **Provas Ilícitas**: interceptações telefônicas, ambientais e gravações clandestinas. 7. ed. São Paulo: Thomson Reuters Brasil, 2019, p. 39.

[249] *Op. cit*, p. 54 e 128.

[250] "A seção 54 da Lei de Polícia de Baden-Württemberg [...] **permite o monitoramento secreto do conteúdo das telecomunicações para fins policiais preventivos** para proteger certos interesses jurídicos importantes. [...] A implementação da chamada vigilância de telecomunicações de origem (fonte TKÜ) [...] pressupõe que o sistema alvo está **infiltrado com software de vigilância**" (Tradução nossa): **BvR 2771/18** (Disponível em: bit.ly/3P7EQhz. Acesso em: 20 out. 2022.

não atendendo aos requisitos de justificação exigidos para tal ação constitucional de discussão suficiente das normas técnicas do direito da União[251].

Com essas leis, o uso de medidas de vigilância policial por meio de *Trojans* estaduais foi ampliado, consideravelmente, em face do combate ao crime de forma mais vasta pela polícia[252].

De qualquer forma, o *hacking* estatal é uma alternativa regulamentada por lei, que alterou o Código de Processo Penal da Alemanha, com estrutura operacional pela polícia em pleno funcionamento, apesar de críticas e eventual reversão pelo Tribunal Constitucional Alemão.

A doutrina encara o *software* de espionagem, nestes moldes da legislação da Alemanha, como um **"método oculto *excepcionalíssimo* de investigação"**[253], pois demasiadamente intrusivo na vida privada do investigado (espionagem em tempo real no fluxo de conversas e amplo acesso a dados do *smartphone*), exigindo detalhamento normativo mais amplo que o da mera interceptação telefônica, como a

> [...] definição dos locais em que o *software* pode ser ativado; as funções a serem executadas; disposições sobre como deve ser feita a documentação de toda a aplicação da medida e dos resultados obtidos; bem como disposições sobre a preservação dos dados angariados, de modo a permitir à defesa o exercício do contraditório no momento oportuno e também verificar a existência de restrição infundada a direitos fundamentais do investigado. Mostra-se também necessária a previsão de controle da aplicação da medida por profissionais desvinculados das autoridades responsáveis por conduzir a investigação, de modo a permitir que sejam inspecionadas e removidas informações sobre o núcleo da vida privada do investigado.[254]

Mais uma vez, assim, verifica-se de toda a base legislativa da Alemanha o posicionamento que também vem se firmando nos EUA, o da regulamentação legislativa, justamente na busca do equilíbrio, da proporcionalidade dos limites do emprego dos direitos e garantias fundamentais:

---

[251] No mesmo sentido de inadmissibilidade da demanda acima, mas do estado alemão de Hesse: **BvR 1552/19**. "Reclamação constitucional malsucedida contra os regulamentos de Hesse sobre acesso secreto a sistemas de tecnologia da informação". Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2022/bvg22-020.html. Acesso em: 20 out. 2022.

[252] In: HAUFE ONLINE REDAKTION. Verfassungsklage gegen neue Abhörmöglichkeiten der Geheimdienste durch Quellen-TKÜ. **Haufe**, 5 jul. 2021. Disponível em: https://www.haufe.de/compliance/recht-politik/verfassungsklage-gegen-online-durchsuchung-mit-staatstrojaner_230132_463812.html. Acesso em: 20 out. 2022.

[253] RIBOLI, Eduardo Bolsoni. **Eu sei o que vocês fizeram no verão passado": o uso de software de espionagem como meio de obtenção de prova penal.** Revista Brasileira de Ciências Criminais, São Paulo, v. 156, p. 91-139, jun. 2019, p. 8.

[254] *Op. cit*, p. 8-9.

> O problema é que, **embora o hacking legal seja definitivamente uma alternativa mais desejável para a restrição de criptografia,** o debate sobre o quão o hacking legal deve ser regulamentado ainda está em seus estágios iniciais. [...]. **Uma estrutura legal robusta para hackers legais é necessária a fim de permitir as atividades de investigação da aplicação da lei, por um lado, e salvaguardar segurança, direitos fundamentais e devido processo, por outro**. Os obstáculos para estabelecer esta estrutura é o que deve ocupar o centro do palco no debate "Going dark".[255] (Tradução e Grifo nossos).

Contudo, apesar de a Corte Constitucional alemã já ter definido como

> um novo direito constitucional a confiabilidade e integridade dos sistemas de tecnologia da informação, de modo a protegê-lo diante de ingerências estatais investigativas que buscassem alcançar o fluxo de informações de maneira oculta utilizando a internet,[256]

por outro lado, estabeleceu critérios para a flexibilização deste direito, entendendo **não ser um direito fundamental absoluto**, "podendo ser restringido para fins **preventivos** ao processamento de ilícitos penais desde que sua restrição seja **proporcional**" [257]; ou seja, a existência de evidências de outros valores igualmente relevantes devem ser protegidos, analisados no caso concreto por decisão judicial.

Mas, é preciso ressaltar que o direito probatório da Alemanha tem sido criticado, pois, apesar de intensos contrapesos do Estado desses país[258], pouco críveis de concretização no Brasil,

> a abordagem jurisprudencial ponderadora entre eficiência investigativa e direitos fundamentais tem causado inevitável insegurança jurídica quanto ao alcance desses últimos, que tendem a ser desprestigiados em casos de grande comoção pública, real ou potencial.[259]

---

[255] Conforme: LIGUORI, Carlos. Exploring Lawful Hacking as a Possible Answer to the "Going Dark" Debate. **Michigan Technology Law Review**, v. 26, n. 317, p. 317-347, 2020. Disponível em: https://repository.law.umich.edu/mtlr/vol26/iss2/5. Acesso em: 30 nov. 2021, p. 344.

[256] In: MENDES, Carlos Hélder C. Furtado. **Tecnoinvestigação criminal**: entre a proteção de dados e a infiltração por software. Salvador: Juspodivm, 2020, p. 230.

[257] *Op.* cit, p. 232.

[258] Como a "prestação de todos os direitos sociais; sua seriedade na imposição de duras sanções disciplinares, cíveis e até criminais aos agentes que, exercendo atividades investigativas, cometem ilegalidades e abusos, e sua relativamente rápida incorporação de precedentes do Tribunal Europeu de Direitos Humanos [...]". (In: SOARES, Gustavo Torres. **Investigação criminal e inovações técnicas e tecnológica**s. Belo Horizonte: D'Plácido. 2020, p. 119-120).

[259] *Op.* cit, p. 119.

Mais recentemente, também ao âmbito estadual da Alemanha, estendeu-se tal previsão legal preventiva, com críticas de igual natureza; normativa pré-delitual que, certamente, se ausente qualquer limite particular do caso concreto, seria inadmitida no ordenamento jurídico brasileiro, ao menos frente aos requisitos da Lei 9296/96, no seu art. 2º, inciso III, pois, exige-se o fato investigado **constituir** infração penal, apesar de nos limites de uma cautelaridade, suficientemente motivados para a demanda específica[260].

O ensinamento que se traz dessa nova toada alemã é, justamente, o cuidado na interpretação da lei voltada à efetivação de uma interceptação telemática preventiva, no sentido de um *Big Brother* do Estado à fiscalização preditiva e em massa, sobretudo em demandas que a nova legislação busca justificativas demasiadamente genéricas ("perigo urgente" e "interesse público"), abarcando terceiros que nada tem a ver com o crime investigado, por condição pessoal de alguma possível correlação.

Apesar de justificativas aceitáveis em casos de extrema urgência de segurança nacional, crimes graves decorrentes de terrorismo, dentre outros de ataque a uma Nação, tais atos de investigação "preventivos" devem ser autorizados pelo magistrado de forma meticulosa, com base na questão específica e sem prejuízo das demais cominações legais, tais como ressalva a Suprema Corte dos EUA quanto às "circunstâncias exigentes", sob pena da ilicitude da prova obtida pela interceptação.

Mas de uma forma geral, como visto, em razão da alteração do CPP alemão, desde 2017 os investigadores do país têm permissão para hackear dispositivos móveis de suspeitos, colocando o *software* de vigilância para ler suas comunicações. E tal poder já foi estendido à polícia federal e a todos os 19 serviços de inteligência federais e estaduais, pois passaram a ter poderes semelhantes calcados em recentes mudanças na Lei de Proteção Constitucional (*Verfassungsschutzgesetz*)[261] e na Lei

---

[260] "Havendo o Juízo de primeiro grau **deferido a gravosa medida unicamente em razão do "esclarecimento dos fatos"**, de o "crime investigado ser punido com pena de reclusão" e de "haver indícios de autoria que mereçam ser investigados", **porém sem demonstrar, diante de elementos concretos,** [...] **quebranta a regra do sigilo**, que [...] **em vez de exceção, tornar-se-ia regra.**" (STJ, HC 150995/PR. Relator: Min. Sebastião Reis Júnior, 6ª Turma. **DJe**, 09 dez. 2015). Grifo nosso.

[261] Lei de cooperação entre os governos federal e estadual em questões relativas à proteção da Constituição e do Departamento Federal de Proteção à Constituição. Tradução nossa. **Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz**. Disponível em: https://www.gesetze-im-internet.de/bverfschg/. Acesso em: 20 out. 2022.

da Polícia Federal (*Bundespolizeigesetz*), as quais foram aprovadas pelo *Bundestag* em 10 de junho de 2021[262].

Extrai-se da referida Lei da Polícia Federal, no título "Poderes Especiais" para a "§ 21 Coleta de dados pessoais"[263]:

> (1) [...] a Polícia Federal poderá coletar dados pessoais [...] (2) Para **prevenir** infrações penais, a coleta de dados pessoais **só é permitida** se os fatos justificarem a suposição de que 1. a pessoa pretende cometer infrações penais [...] de **considerável importância e os dados são necessários para prevenir tais infrações penais** ou 2. a pessoa está em contato com uma pessoa nomeada no número [...] e **isso seria inútil ou significativamente mais difícil em qualquer outra maneira**. (Tradução nossa).

E, conforme o § 28 dessa lei,

> (3) Exceto em caso de **perigo iminente**, o uso de meios especiais [de coleta de dados] [...] só poderá ser ordenado pelo **chefe da autoridade policial federal** [e em certos casos definidos na lei e prazo limitado a um mês]. **A prorrogação da medida exige um novo pedido [com decisao proferida] pelo juiz** [...]. (4) Os documentos obtidos [...] devem ser **destruídos imediatamente se não forem necessários** para os fins em que se baseia o despacho ou de acordo com o Código de Processo Penal para o processo de uma infração penal. (Tradução e grifo nossos).

Em vista dessas reformas, a Polícia Federal[264], diretamente (ou, após decisão de um magistrado), também poderá monitorar (hackear) preventivamente as comunicações das pessoas, sob os requisitos previstos em lei (cabendo as mesmas observações acima expostas): que se trate de evitar um perigo urgente para a existência ou segurança do governo federal ou de um estado ou para a vida, integridade ou liberdade de uma pessoa ou propriedade de valor significativo, cuja preservação é no interesse público, com a possível extensão investigativa a pessoas do contato dos suspeitos, nas circunstâncias previstas em lei[265]. Neste caso, prevê a lei alemã a regra supletiva do meio probatório para a interceptação a terceiros (contatos dos suspeitos) se não houver outro meio investigativo viável, conforme também prevista na legislação brasileira (Lei n. 9296/96, art. 2º, inciso II: " Não será

---

[262] BEUTH, *Op. cit*.

[263] Lei da Polícia Federal. **Gesetz über die Bundespolizei (Bundespolizeigesetz - BPolG).** Disponível em: https://www.gesetze-im-internet.de/bgsg_1994/BJNR297900994.html. Acesso em: 20 out. 2022.

[264] *Op. cit*.

[265] Tal como nos comentários do subcapítulo 3.1.5.2.2, quanto à lei de Utah (H.B. 57/2019) e a questão das exceções em caso de "circunstâncias exigentes": "(2) (a) "Uma agência de aplicação da lei pode obter **informações de localização sem um mandado para um dispositivo eletrônico**".

admitida a interceptação de comunicações telefônicas quando ocorrer qualquer das seguintes hipóteses: II — a prova puder ser feita por outros meios disponíveis;").

Do ponto de vista prático, também outro ponto merece atenção. Inobstante a possibilidade do *hacking* legal, a polícia alemã vem aplicando com êxito operacional técnica investigativa diversa, inclusive de conversações em tempo real através de sistemas que adotam a criptografia ponta a ponta, com maior repercussão na mídia das realizadas através do WhatsApp Web[266]. E

> o principal meio de obtenção de prova utilizado é a **infiltração** (ou pesquisa) ***online*** em razão de se obter um verdadeiro *Big Brother* da vida do investigado: "**fornece acesso aos dados que já estão armazenados no computador ou telefone celular do interessado.** [...] **permite que as agências de aplicação da lei acessem documentos, fotos, vídeos e outros arquivos armazenados.** [...] **que o microfone e a câmera do computador ou telefone sejam ligados, para gravar imagens e sons em torno do suspeito.** [267] (tradução e grifo nossos).

E aqui há uma divergência brasileira por decisão de importante julgado do Superior Tribunal de Justiça, difícil de ser superado por seus precisos e lógicos argumentos, exceto por lei regulamentando o procedimento e alguma possibilidade tecnológica de obediência aos ditames legais da cadeia de custódia para possibilitar o devido processo legal ao acusado. Tecnicamente, deve-se disciplinar a devida produção da prova digital, mesmo se dotados da E2EE,

> pois, quando não submetidos a softwares que realizem o espelhamento e a correta extração dos dados: 1) será possível a exclusão de mensagens pelo método 'apagar para mim' de remetentes e destinatários, sendo possível manipular cenários; 2) eventuais modificações poderão ser realizadas de forma irrastreável, inclusive em 'modo avião'; 3) eventuais atos derivados do manejo livre, como a realização de prints, acarretarão a modificação do status do smartphone em relação ao momento da sua apreensão. [268]

---

[266] O BKA consegue monitorar a comunicação via WhatsApp Web há vários anos "mesmo sem ter que instalar um software de monitoramento no celular do destinatário [por] método que permite que mensagens curtas de texto, vídeo, imagem e voz [...] sejam rastreadas em tempo real" (Tradução e grifo nossos. Vide: FLADE, Florian; TANRIVERDI, Hakan. BKA kann bei WhatsApp mitlesen. **Tagesschau**, 21 Juli 2020. Disponível em: bit.ly/3Y0qiEw. Acesso em: 10 maio 2021).

[267] In: PORTNER, Léo. Kann die polizei ihre WhatsApp-, viber- oder Facebook-Nachrichten lesen? **Dr. Miluscheva**. Disponível em: https://www.bg-anwalt.de/infothek/strafrecht/kann_die_polizei_ihre_whatsapp_viber_oder_facebook_nachrichten_lesen.html. Acesso em: 06 dez. 2021.

[268] EBERHARDT, Marcos; PIPPI, Marcos. Prova criminal: WhatsApp e cadeia de custódia. **Consultor Jurídico**, 13 out. 2021. Disponível em: https://www.conjur.com.br/2021-out-13/eberhardt-pippi-prova-criminal-whatsapp-cadeia-custodia?s=08 . Acesso em: 07 dez. 2021.

Em vista dessas problemáticas, o Colendo STJ[269] já entendeu ser inadmissível a prova obtida através do espelhamento do WhatsApp Web do investigado, por eventual possibilidade de alteração pelo órgão investigativo das conversas entre o usuário do celular e terceiros com quem conversou, já que o policial poderia apagar ou adicionar diálogos atuais e passados, sem deixar vestígios, por causa da criptografia ponta a ponta do WhatsApp resultar no ausente *backup* no servidor da empresa. Ou seja, não haveria possibilidade de perícia, decorrendo uma indevida presunção absoluta da legitimidade dos atos dos investigadores e a produção de prova diabólica pelo acusado. Entendeu-se, assim, descaber a analogia para aplicação da Lei n. 9296/96, diferindo desta o "espelhamento", porque o policial pode não se comportar como mero observador dos interlocutores, por possibilitar acesso a conversas anteriores ao espelhamento e pelo fato de a prévia apreensão do celular do investigado, como demanda impositiva para a leitura do QR *code* para o uso do WhatsApp Web, dever dar-se antecipadamente por autorização judicial, o que não ocorreu no caso concreto. Decidiu-se no Acórdão pela nulidade da decisão judicial que autorizou o espelhamento do WhatsApp via Código QR, bem como das provas e dos atos que dela diretamente dependam ou sejam consequência, ressalvadas eventuais fontes independentes; com isso, a prisão preventiva dos investigados foi revogada.

Uma observação crítica para este julgado, sem contar com as demais ilegalidades apontadas no Acórdão, mas focando na ideia central de que o conteúdo das conversas do investigado via WhatsApp Web poderia ser alterado pelo policial, é a possibilidade de produção de provas que seriam irrefutáveis serem de produção material somente pelo acusado (ato personalíssimo) através de seu celular, como fotografias, áudios e vídeos nos quais se identifica ele próprio cometendo o fato delituoso, a vítima em alguma situação degradante, ou, fotos do local dos fatos criminosos com indícios ou objetos e instrumentos do crime, por exemplo. Excluir, de

---

[269] Vide: BRASIL. Superior Tribunal de Justiça. RHC 99.735. Relatora: Min. Laurita Vaz. **Diário de Justiça Eletrônico**, Brasília, DF, 12 dez. 2018.

plano[270], a prova digital produzida dessa maneira, portanto, não deve ser o paradigma do precedente judicial sob o fundamento central de manipulação pela polícia[271].

Outro fator que deve ser levantado é continuar a pesquisa científica para investigar alguma tecnologia ou solução da polícia alemã que, talvez, o público ainda desconheça, dada a expressa retenção de informações estratégicas de como opera em tais meios investigativos, como noticia a imprensa em várias fontes pesquisadas ora citadas. E não se descarta que a polícia alemã não dê primazia a atos investigativos preventivos, sem focar (ou se importar) na produção de prova admissível futura para um processo-crime, mas a atos de controle policial (de "inteligência"), como já destacado logo acima, com fundamento no "perigo urgente" e "interesse público", principalmente em atos de terrorismo e de segurança nacional, tal como se verificou ocorrer nos EUA.

Apesar das críticas, e, pendente a decisão pela Suprema Corte da Alemanha, esta valorização da "taxatividade" (lei escrita advinda do Parlamento, tanto no âmbito federal, quanto estadual) em complemento às regras de interceptação telefônica e telemática já presentes em seu Código de Processo Penal[272], foi a opção mais acertada, já que se ausente regras claras do agir das forças estatais de investigação e a prévia delimitação de regras de procedimento[273] para evitar provas ilícitas ou inviáveis de perícia para a contraprova pela Defesa do investigado resultará, provavelmente, na ineficiente persecução penal e o descrédito da Justiça.

Como visto no julgamento do STJ pouco acima citado, esse foi o outro fundamento para afastar a prova produzida, pois se afastou a analogia com a Lei de

---

[270] "**A violação da cadeia de custódia** [...] **não implica, de maneira obrigatória, a inadmissibilidade ou a nulidade da prova colhida**." (BRASIL. Superior Tribunal de Justiça. **Quebra da cadeia de custódia não gera nulidade obrigatória da prova, define Sexta Turma**. Brasília, 9 dez. 2021. Disponível em: bit.ly/3utow1b. Acesso em: 12 dez. 2021).

[271] Como motivado no subcapítulo 4.2, houve recente julgado em sentido diverso do que se estava entendendo no STJ quanto à validade probatória de *prints* de conversas digitais via WhatsApp, passando a admitir, diante das peculiaridades do caso, seu uso como prova válida para condenação, e, que caberia à defesa demonstrar sua inidoneidade (STJ, AgRg no HC 752.444/SC).

[272] A respeito do Código Processual Penal e dos requisitos até então necessários à interceptação telefônica e telemática alemã, vide: ROXIN, Claus. **Derecho Procesal Penal**. Tradução: Castellana de G. Córdoba y D. Pastor. Buenos Aires: Editores del Puerto, 2000, p. 306-312.

[273] Assim, com base na regra da proporcionalidade: "Não há margem para a admissão de medidas restritivas de direitos fundamentais sem expressa previsão legal ou com previsão legal deficiente, que não estabeleça as hipóteses em que a medida poderá ser adotada, os requisitos para sua admissão e o procedimento a ser observado" – Cf.: LOPES, Anderson B. **Os conhecimentos fortuitos de prova no processo penal**. Belo Horizonte: D'Plácido, 2016, p. 110-111.

Interceptação Telefônica (Lei n. 9296/96) no caso do espelhamento do WhatsApp Web.

Também por isso parece ser a criação de leis a preferência atual preconizada nos Estados Unidos da América[274] quanto ao tratamento da produção de provas digitais, mesmo por sua tradição ao *common law*, como concluído na subseção anterior, e, um tratamento jurídico mais adequado a novas estratégias investigativas[275] ser imperativo no ordenamento jurídico brasileiro[276].

---

[274] E "O **critério de interpretação do contexto transnacional** não pode simplesmente decretar a falência do **princípio da taxatividade**, o que faria com que a forma fosse reconduzida **a um sistema judicial (inclusive supranacional)** de controle sobre os atos processuais." (GLOECKNER, Ricardo Jacobsen. **Nulidades no Processo Penal**. 3. ed. São Paulo: Saraiva, 2017, p. 269; grifo nosso).

[275] Um bom referencial para garantir a integridade e autenticidade da prova digital produzida são as regras da ABNT NBR ISO/IEC 27037:2013 (ISO 27037 Diretrizes para identificação, coleta, aquisição e preservação de evidência digital. **Academia de Forense Digital**, jan. 2019. Disponível em: https://academiadeforensedigital.com.br/iso-27037-identificacao-coleta-aquisicao-e-preservacao-de-evidencia. Acesso em: 20 out. 2022).

[276] Além disso, estabelecer prévias regras de extração da prova digital, baseada nas legislações e precedentes judiciais já fixados no Brasil e no exterior, resultariam numa "coerência fática e normativa" (vide: MACCORMICK, Neil. **Argumentação jurídica e teoria do direito**. São Paulo: Martins Fontes, 2006, p. 197) para seu uso interno e a pedido de outras Nações.

4 O BRASIL E A PRODUÇÃO DA PROVA PENAL DIGITAL CRIPTOGRAFADA: STF E LEGISLAÇÃO POSTA E PROPOSTA

4.1 A SITUAÇÃO NO ORDENAMENTO JURÍDICO BRASILEIRO

Iniciando-se o estudo mais incisivo da realidade do Brasil, especialmente quanto ao tema proposto da interceptação telemática de mensagens digitais dotadas de criptografia de ponta a ponta à investigação criminal, imprescindíveis são as análises em todas as frentes possíveis: jurisprudencial (especialmente no STF), além da ordem legal vigente e de propostas de lei em trâmite no Congresso Nacional.

Do estudo de questões teórico-práticas provenientes de artigos científicos de diversos delegados e investigadores de polícia[277] brasileiros especializados em crimes cibernéticos, concluiu-se, tal como já constatado no estudo do direito comparado, a impossibilidade, com a tecnologia atual ao menos, da produção da prova penal digital[278] através da interceptação telemática em face da E2EE, disponível em diversos aplicativos de mensageria privada; exceto por meios alternativos, como um cavalo de Tróia instalado pela polícia diretamente no celular, dentre outras maneiras, ressaltando os especialistas que, em regra, dependeriam da senha pessoal no aparelho celular para seu completo acesso, evidentemente, negada pelo acusado de crimes graves abrangidos pela Lei n. 9296/96.

As informações da investigação criminal em tais casos são de extrema valia ao deslinde de crimes, já que, por exemplo,

> [...] por intermédio da interceptação telemática de WhatsApp, será possível saber os números de telefone dos interlocutores do investigado (em poder dessa informação é possível obter informações do WhatsApp e de operadoras sobre cada um deles), esclarecer os tipos de conteúdo que foram enviados durante as conversas (exemplos: texto, figura, vídeo etc.), receber informações sobre tipo de dispositivo, datas, horários, endereçamentos IP e

---

[277] Cf.: **a)** ALVES, Gustavo André; LOURENÇO, Marcus Vinicius. Extração de Mensagens do Aplicativo WhatsApp (p. 163-174); **b)** KONNO JÚNIOR, Janio. Interceptação Telemática ou Busca e Apreensão de Dados em Nuvem e a Preservação da Cadeia de Custódia (p. 273-287). In: JORGE, Higor Vinicius Nogueira (Coord.). **Tratado de Investigação Criminal Tecnológica**. 2. ed. Salvador: JusPodivm. 2021.

[278] Nos termos do art. 25 da Lei de Abuso de Autoridade (n. 13.869/19) e preceitos de obediência à cadeia de custódia das provas.

> portas lógicas de cada conversa que o investigado manteve e outras informações relevantes para investigação criminal. [279].

O que resta à investigação criminal ao menos até este momento, então, é a busca investigativa policial por outros meios probatórios, como o fornecimento de metadados em e-mails, fotos, vídeos, dentre outras informações dispostas em nuvem (Google Drive, Apple iCloud etc.), através de pedidos diretos a tais provedores (art. 13-A do CPP; art. 17-B da Lei 9613/98; art. 15 da Lei 12.850/13) e, judicialmente, por mandados de busca e apreensão de dados armazenados nos servidores (arts. 240 e seguintes do CPP)[280], além da própria interceptação telemática de comunicações digitais em fluxo, quando possível pela tecnologia existente, como especificado no art. 7º, incisos I a III, do Marco Civil da Internet[281] e jurisprudência do STJ[282].

Aliás, imperiosa uma cautela quanto aos precedentes judiciais tidos como verdades absolutas nas questões criminais. Como já demonstrado em diversas passagens deste estudo, dada uma infinidade de situações possíveis do caso em concreto, a sentença penal é atividade artesanal, particular e diferenciada por suas singularidades do ocorrido e das provas produzidas, valendo à pena a transcrição do julgado a seguir, que se utilizou inclusive do conceito norte-americano da "expectativa razoável de privacidade", inexistente quanto ao acesso à fotografia (dado) contida em celular abandonado sem autorização judicial, mantida a cláusula constitucional de reserva da jurisdição para o sigilo telefônico:

> HABEAS CORPUS. ROUBO MAJORADO. ACESSO A TELEFONE CELULAR ENCONTRADO EM VEÍCULO ABANDONADO. ALEGAÇÃO DE ILICITUDE DA PROVA COLHIDA. NÃO OCORRÊNCIA. FOTOGRAFIA. EXPECTATIVA DE PRIVACIDADE. INEXISTÊNCIA. HABEAS CORPUS

---

[279] WENDT, Emerson; JORGE, Higor Vinicius Nogueira. Interceptação Telemática de Contas do WhatsApp (bilhetagem – extrato de mensagens) – versão 2019.4 (p. 139-145), p. 141. In: JORGE, Higor Vinicius Nogueira (Coord.). **Tratado de Investigação Criminal Tecnológica**. 2. ed. Salvador: JusPodivm. 2021.

[280] "II - O acesso ao conteúdo armazenado em telefone celular ou smartphone, **quando determinada judicialmente** a busca e apreensão destes aparelhos, não ofende o art. 5º, inciso XII, da Constituição da República, porquanto **o sigilo [...] é em relação à interceptação telefônica ou telemática propriamente dita, ou seja, é da comunicação de dados, e não dos dados em si mesmos**." (STJ, 5ª Turma, RHC 75800/PR. Relator: Min. Felix Fischer. Julgado em: 15/09/2016. **DJe**, 26 set. 2016).

[281] "Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I - inviolabilidade da intimidade e da vida privada, [...]; II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;" (MCI).

[282] O STJ vem decidindo que "é ilícita a tomada **de dados, bem como das conversas** de Whatsapp, obtidas diretamente pela autoridade policial em aparelho celular apreendido no flagrante, sem prévia autorização judicial. [é] o ônus de comprovar a higidez dessa autorização [acesso ao aplicativo pelo acusado], com prova da voluntariedade do consentimento, recai sobre o estado acusador." (STJ, HC 674185/MG. Relator: Min. Sebastião Reis Júnior. Julgado em: 17 ago. 2021. **DJe**, 20 ago. 2021).

> PARCIALMENTE CONHECIDO E, NO MAIS, DENEGADO. 1. No que tange à jurisprudência desta Corte Superior sobre o acesso pela polícia de telefone celular de acusado sem mandado judicial, forçoso lembrar que, por ocasião do **julgamento do RHC n. 51.531, precedente paradigmático quanto ao tema, esta Sexta Turma enfatizou a necessidade de uma análise casuística, ante a impossibilidade de esgotar-se a complexidade do tema em um único julgado.** 2. A impetração invoca precedente desta Sexta Turma, o HC n. 418.180, em que foi concedida a ordem, "a fim de reconhecer a ilegalidade das provas produzidas pelo acesso aos telefones celulares sem mandado judicial". Todavia, **não há similaridade entre o caso daqueles autos com o ora analisado**. No HC n. 418.180, o acusado foi preso em flagrante e, da "análise dos aparelhos telefônicos apreendidos em posse dos flagranteados permitiu-se a identificação e envolvimento dos demais investigados, apontando, desse modo, indícios veementes de que integram organização criminosa dedicada ao tráfico internacional de drogas". Na espécie, **nenhum aparelho foi apreendido em decorrência de prisão em flagrante, mas de apreensão de carro abandonado. Ou seja, o aparelho celular estava igualmente abandonado. Forçoso concluir que o âmbito de proteção da norma que protege a intimidade não é a mesma nos dois casos**. 3. Os depoimentos dos policiais que encontraram a res furtiva indicam que o telefone celular — origem da fotografia de outro veículo, que, pela placa, viabilizou a localização do paciente e objeto da tese defensiva de violação de sigilo — estava dentro do automóvel abandonado, de modo que, tratando-se de *res derelictae*, não estava albergado pela proteção invocada pela defesa. 4. O alegado constrangimento ilegal **não decorre do acesso a comunicações telefônicas — proteção constitucional que não poderia ser relativizada em função de o telefone estar abandonado** — e, dada a **reduzida expectativa de privacidade** inerente à condição do telefone, abandonado com o veículo em local público, forçoso concluir **não haver ilicitude no acesso à fotografia** em questão. 5. O **direito comparado** informa que, para reconhecer-se violação de legítima expectativa de privacidade, a ação governamental deve infringir a privacidade de um indivíduo que, efetivamente, efetuou esforços razoáveis para protegê-la, bem como tal expectativa deve ser razoável, no sentido de que a sociedade em geral a reconheceria como tal. [...] 7. Habeas corpus parcialmente conhecido e, no mais, denegado. (STJ, HC 552455/ES. Relator: Min. Rogério Schietti Cruz, 6ª Turma, julgado em 09 mar. 2021. **DJe**, 17 mar. 2021).

Sem prejuízo dessas possibilidades investigativas atuais, todavia, segue a pressão social e de autoridades, exposta desde o início deste estudo: uma tentativa voraz do resguardo da segurança pública, sob o argumento da impunidade do acusado e que o seu direito ao sigilo de mensageria digital dotado de criptografia ponta a ponta não é absoluto. Por conta disso, observa-se um esforço do Poder Legislativo de todo o mundo; e no Brasil não é diferente, porquanto há forte movimento para normatizar, por diferentes frentes, a produção da prova penal digital dotada da E2EE.

Numa análise mais global, há precedente advindo da Corte Interamericana de Direitos Humanos (CIDH), denominado como "Caso Escher e Outros vs. Brasil" (julgado em 2009)[283], no qual o Estado foi condenado pela interceptação, gravação e

[283] CORTE IDH. Caso Escher e Outros *vs.* Brasil, de 6 de julho de 2009. Disponível em: www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf. Acesso em: 17 nov. 2022.

divulgação das conversas telefônicas dos interessados, constando no voto como um dos objetivos da Corte o aperfeiçoamento da jurisprudência interamericana sobre a tutela do direito à privacidade e do direito à liberdade de associação, assim como os limites do exercício do poder público.

O núcleo relevante desta decisão é a caracterização da fluidez da comunicação telefônica por sistemáticas inovações da tecnologia, consignando-se que **não existe direito absoluto à privacidade dos cidadãos**, ressalvado o abuso do Estado (arbitrariedade), cumulada com a exigência de previsão e obediência da lei para a devida interceptação telefônica, necessária e proporcional (por motivação judicial idônea), visando a um fim democrático e legítimo. Enfatize-se do precedente a força-normativa no ordenamento jurídico brasileiro da CADH[284] e a relevância trazida, por conseguinte, de uma decisão da CIDH, especialmente, no seguinte ponto do julgado:

> 115. A fluidez informativa que existe atualmente coloca o direito à vida privada das pessoas em uma situação de maior risco, devido à maior quantidade de novas ferramentas tecnológicas e à sua utilização cada vez mais frequente. Esse progresso, especialmente quando se trata de interceptações e gravações telefônicas, não significa que as pessoas devam estar em uma situação de vulnerabilidade frente ao Estado ou aos particulares. Portanto, o Estado deve assumir um compromisso com o fim adequar aos tempos atuais as fórmulas tradicionais de proteção do direito à vida privada.
> 116. Inobstante, conforme se depreende do artigo 11.2 da Convenção[285], o direito à vida privada não é um direito absoluto e, portanto, pode ser restringido pelos Estados quando as ingerências não forem abusivas ou arbitrárias; por isso, devem estar previstas em lei, perseguir um fim legítimo e ser necessárias em uma sociedade democrática.
> [...]
> 139. Em ocasiões anteriores, ao analisar as garantias judiciais, o Tribunal ressaltou que as decisões adotadas pelos órgãos internos que possam afetar direitos humanos, devem estar devidamente motivadas e fundamentadas, caso contrário, seriam decisões arbitrárias.

Voltando ao ponto de vista normativo, técnica especial de investigação voltada à produção de prova da prática de crimes foi sacramentada no âmbito internacional (Convenção de Palermo ou Convenção das Nações Unidas contra o Crime

---

[284] O STF já decidiu que os tratados e as convenções internacionais sobre direitos humanos podem ser incorporados como emenda constitucional, ou, possuem status de normas supralegais (abaixo da Constituição Federal), retirando a eficácia de todo o ordenamento infraconstitucional em sentido contrário. (Tema 60 do STF).

[285] "Artigo 11. Proteção da honra e da dignidade: 2. Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação". (CADH).

Organizado Transnacional[286], incorporada no Brasil no Decreto n. 5.015/2004) e regulamentada em diversas leis no ordenamento jurídico do Brasil: a infiltração virtual de agentes da polícia[287], para crimes praticados através da *internet*, após prévia autorização judicial. Há também uma gama de leis nacionais: Lei n. 9034/95 (art. 2º, V), revogada pela Lei n. 12850/13; Lei 11343/06, art. 53, I; Lei n. 12850/13, art. 3º, VII; Lei n. 13.441/17 (arts. 190-A a 190-E, todos do ECA); Lei n. 13964/19 (arts. 10-A a 10-D da Lei 12850/13), apontadas pela doutrina como um microssistema nacional coordenado ao plano internacional[288] para sua aplicação, tal como preconizado pela Convenção de Budapeste.

Essa prática investigativa policial da infiltração virtual não abarca todas as situações necessárias, todavia[289]. Apesar de sua relevância e possa ser aplicada em situações práticas correlatadas, não se confunde com os objetivos de uma interceptação telemática abrangendo terceiros envolvidos. Permanece ausente legislação específica para o caso da interceptação telemática de mensagem dotada da E2EE e, em virtude dessa necessidade social, os juízes acabaram tendo que enfrentar esta polêmica por todo o país, resultando na determinação de suspensão do aplicativo WhatsApp em todo o Brasil, multas diárias e até pedidos de prisões dirigidos a representantes de aplicativos dotados de criptografia ponta a ponta que não forneciam tais dados, pretensões cessadas por decisões do STF e do STJ.

Em casos de deferimento por decisão judicial de interceptação telemática em tempo real, autoridades policiais têm relatado dificuldades técnicas no seu

---

[286] Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/decreto/d5015.htm. Acesso em 19 set. 2022. Em destaque seu art. 20: "1. [...] cada Estado Parte [...] adotará as medidas necessárias [...] e **o recurso a outras técnicas especiais de investigação**, como a **vigilância eletrônica ou outras formas de vigilância e as operações de infiltração**, por parte das autoridades competentes no seu território, a fim de combater eficazmente a criminalidade organizada." (Grifo nosso).

[287] PIMENTEL, Fabiano. **Provas, procedimentos e recursos criminais**. Belo Horizonte; São Paulo: D'Plácido, 2020, p. 114. Em comentários ao art. 10-A da Lei n. 12.850/13, preleciona a doutrina que se trata "[...] de uma infiltração de agentes policiais, com o objetivo de combater crimes realizados na rede mundial de computadores, com os mesmos requisitos e prazos para a infiltração de agentes no ambiente real."

[288] SATO, Gustavo Worcki. A Infiltração Virtual de Agentes e o Combate à Pedopornografia digital. In: JORGE, Higor Vinícius Nogueira (Org.). **Direito Penal sob a Perspectiva da Investigação Criminal Tecnológica**. São Paulo: JusPodivm, 2021, p. 506.

[289] Os limites de atuação do policial infiltrado (presencial) podem ser utilizados como parâmetro na virtual, especialmente, um atuar dentro dos limites constitucionais, quando, havendo necessidade investigativa posterior à primeira decisão judicial (v.g. a captação e gravação de conversas), uma nova deverá ser requerida. Cf.: SOUZA, Sérgio Ricardo de. **Prova penal e tecnologia**: novas técnicas e meios de investigação e captação de provas. Curitiba: Juruá, 2020, p. 365.

cumprimento, pois apesar do deferimento inicial de pedido de aplicação de multas, restaram pacificadas como incabíveis pelo Poder Judiciário (assim como tais suspensões de funcionamento do WhatsApp pelo STF nas ADPF 403 e ADI 5527), no caso da criptografia ponta a ponta em face do argumento da impossibilidade técnica de cumprimento. Sobressai-se o entendimento do STJ, com menção ao precedente paradigmático desta Corte[290]:

> PROCESSO PENAL. AGRAVO REGIMENTAL NO RECURSO EM MANDADO DE SEGURANÇA. INTERCEPTAÇÃO DE DADOS. DESCUMPRIMENTO DE ORDEM JUDICIAL. ASTREINTES. CABIMENTO. INVIOLABILIDADE DO SISTEMA DE CRIPTOGRAFIA DE PONTA A PONTA. IMPOSSIBILIDADE FÁTICA DE CUMPRIMENTO DA ORDEM JUDICIAL. AGRAVO DESPROVIDO.
> **1. A Terceira Seção do STJ, ao ponderar o conflito entre os direitos à privacidade, à inviolabilidade da comunicação privada, o direito à proteção e à segurança dos dados pessoais, firmou o entendimento de que:** a) não há determinação legal ou da Suprema Corte acerca da necessidade de suspensão do feito enquanto se aguarda o julgamento da ADPF n. 403 e ADI n. 5.527 pelo STF; b) é possível a aplicação, em abstrato, de multa cominatória por descumprimento ou cumprimento a destempo de ordem emanada em processo judicial criminal; e **c) deve ser afastada a multa aplicada ante a impossibilidade fática decorrente de criptografia intransponível, sendo certo que os benefícios advindos da criptografia de ponta a ponta se sobrepõem às eventuais perdas pela impossibilidade de se coletar os dados das conversas dos usuários da tecnologia (RMS n. 60.531/RO, relator Ministro NEFI CORDEIRO, relator para acórdão Ministro RIBEIRO DANTAS, TERCEIRA SEÇÃO, julgado em 9/12/2020, DJe 17/12/2020).**
> 2. Agravo regimental desprovido.

Há informação[291] de que "[...] o Google tem se recusado a promover a interceptação em tempo real, com a alegação de impossibilidades técnicas, tendo fornecido, apenas, após o término da interceptação, cópia de todo o conteúdo gerado" [292], apesar da extrema importância das informações práticas que atos de investigação em face de dados armazenados junto ao Google podem fornecer à persecução penal, como: os atinentes à localização (Google Maps), histórico de pesquisas e curtidas no Google e no Youtube, imagens armazenadas no Google Fotos, dados do Google Drive

---

[290] STJ, AgRg no RMS 56815/RO, rel Min. Antonio Saldanha Palheiro, 6ª Turma. Julgado em: 14 set. 2021. **DJe**, 22 set. 2021.

[291] É possível a criação de "contas espelho" nos e-mails de investigados, "duplicatas onde toda a comunicação feita nas originais apareceriam em tempo real" (GHEDIN, Rodrigo. **Google é multado por não interceptar e-mails durante a Operação Lava Jato da Polícia**. Disponível em: https://gizmodo.uol.com.br/google-emails-lava-jato/. Acesso em: 29 nov. 2022.

[292] Cf.: FREITAS JÚNIOR, Adair Dias de; JORGE, Higos Vinícius Nogueira; GARZELLA, Oleno Carlos Faria. **Manual de Interceptação Telefônica e Telemática**. 2. ed. São Paulo: JusPodivm, 2021, p. 124.

(abrangendo backup de conversas do WhatsApp), dados do Gmail e endereços IP, além de informações de voz e áudio utilizados pelo usuário[293]. E, aplicável o disposto no art. 11, § 2º, do MCI[294], ou seja, descabida alegada impossibilidade jurídica pela empresa, ao menos neste aspecto.

Cabe ainda ilustrar, justamente pela dificuldade probatória penal digital, que as autoridades têm se valido inclusive da participação da população em denunciar crimes cibernéticos (similar à difundida vigilância comunitária de vizinhos), e, do setor privado, como realiza a Safernet Brasil, entidade sem fins lucrativos que vem se destacando no combate a crimes cometidos pela internet contra crianças e adolescentes e bem demonstra em seus dados estatísticos o caráter globalizado do problema[295].

Em síntese do exposto, é fato que, mesmo diante da rede normativa e de proteção hoje existentes, permanece o cenário de vácuo na produção da prova penal digital, notadamente a dotada de E2EE. Nossa Suprema Corte (e os tribunais por todo país) estão se deparando com questões inéditas relativas às provas decorrentes de investigações criminais por inovações tecnológicas, valendo-se dos ditames constitucionais e legais vigentes, mas agora, tendo-se que se basear em conhecimentos técnicos, ainda que básicos, obtidos, inclusive, através de audiências públicas[296].

Destarte, a realidade brasileira é praticamente a mesma de países como os Estados Unidos, Reino Unido e Alemanha: problemas práticos e jurídicos decorrentes da mesma origem pela identidade no uso de aplicativos e plataformas digitais por bilhões de usuários. Cada Nação com similitudes e diferenças entre si merecem estudo comparativo não só por conta de aprendizado através da troca de tecnologias de investigação, mas de experiências e questionamentos de diferentes frentes (autoridades policiais, Legislativo e Judiciário, universidades etc.) e até possíveis

---

[293] *Op.* cit, p. 125-126.

[294] Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de **comunicações por provedores de conexão e de aplicações de internet** em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira [...]. § 2º [...] **mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro** [...].” (MCI).

[295] “Em 16 anos, a SaferNet recebeu e processou 4.441.595 denúncias anônimas, envolvendo 935.496 páginas (URLs) distintas escritas em 10 idiomas e hospedadas em 86.098 domínios diferentes [...] atribuídos para 108 países em 6 continentes” (DATASAFER. **35.057 Atendimentos e 4.441.595 Denúncias.** Disponível em: https://indicadores.safernet.org.br/indicadores.html. Acesso em 19 set. 2022).

[296] Conforme rodapé n. 45.

acordos entre o Poder Executivo e o setor privado (*Big Techs*). Tudo isso também em razão de uma crescente necessidade de transnacionalidade na cooperação de provas, aderindo estes três países e o Brasil à Convenção de Budapeste. Almejam os diversos países estudados, a olhos vistos, estancar falha persecutória penal que vem beneficiando criminosos, nos casos de mensagens digitais criptografadas de ponta a ponta, justamente pela louvável busca de provas sem esquecerem-se das garantias e direitos fundamentais dos cidadãos.

Em seguida, portanto, cogente o foco no estudo pormenorizado das ações constitucionais em andamento no STF e os projetos de lei voltados a sanar essa lacuna resultante da E2EE.

4.2 O STF E A PENDÊNCIA DO JULGAMENTO DAS ADPF 403 E ADI 5527: EXAME CRÍTICO EM FACE DO DIREITO COMPARADO

O caso concreto específico da E2EE já restou judicializado no STF (ADPF 403 e ADI 5527). E, apesar de muito questionável sua eficácia para cumprimento nos EUA[297], o Brasil possui certa relevância sócio-política mundial, além da inerente repercussão natural de uma decisão judicial da mais alta Corte do Brasil, país com o maior número de usuários do WhatsApp do mundo.

Inicialmente, deve-se mencionar que, no Brasil, a complexidade do assunto não é menor quando comparada aos demais países já reportados nesta dissertação, tendo em vista as recentes reformas processuais penais (v.g. os artigos 158-A e 158-B[298], ambos do CPP) e várias outras propostas legislativas em trâmite, conforme à frente será analisado. Há, também, jurisprudência ainda divergente em certos pontos, sem falar da criação de novos tipos penais[299] de modo constante, e de possuirmos, diversamente de países como os EUA, o Reino Unido e a Alemanha, uma polícia

---

[297] Conforme rodapé n. 70.

[298] Sobre as provas digitais: **a)** MACHADO, Vitor P.; JEZLER JUNIOR, Ivan. A prova eletrônica-digital e a cadeia de custódia das provas: uma (re)leitura da Súmula Vinculante 14. **Boletim IBCCRIM**, São Paulo, n. 288, nov./2016; **b)** FURLANETO NETO, Mário; SANTOS, José E. L. dos. Apontamentos sobre a cadeia de custódia da prova digital no Brasil. Disponível em: https://revista.univem.edu.br/emtempo/article/view/3130. Acesso em: 26 jun. 2021.

[299] Arts. 154-A; 155, § 4º-B e § 4º-C; 171, § 2º-A e § 2º-B; 266, § 1º; 298, parágrafo único; todos do Código Penal brasileiro, com destaques aqui de recente alteração pela Lei n. 14.155, de 27 de maio de 2021.

defasada em equipamentos e peritos[300] para demanda necessária à crescente produção da prova digital[301]:

> A capital [Curitiba-PR] acumula 90% dos requerimentos do estado, já que nem todos os exames são realizados pelos laboratórios do interior. **Na tarde de terça-feira (17), eram 17.406 materiais pendentes na fila da perícia**, segundo consulta realizada no *site* do Instituto de Criminalística. [...] **A análise de material extraído de cada telefone celular, trabalho feito por peritos, dura, em média, seis horas. Já a análise de dados de computadores leva cerca de 30 horas de perícia**. [...] **a demanda cresce vertiginosamente no setor de computação forense**. Um levantamento do sindicato afirma que são necessários pelo menos 17 peritos no laboratório de Curitiba para atender a demanda. Para dar conta dos mais de 17 mil materiais na fila, seriam necessários ao menos 32 peritos[...]. A capital recebe entre 10 ou 12 ofícios por dia, alguns com mais de um material para análise.[302]

Para demonstrar a relatada dificuldade quanto aos precedentes, em não poucos casos as conclusões do STJ e do STF, acerca das provas obtidas em aparelhos de celular ou microcomputadores, são divergentes e instáveis no âmbito processual penal, repercutindo numa dificuldade de julgamento por todo o país[303], e, a criticável ineficiência ao Poder Judiciário no exame de novas tecnologias que dependam de prova pericial fidedigna[304], tal como declararam os juízes da Suprema Corte norte-americana[305] no caso Jones.

Apesar dessas instabilidades quanto aos precedentes judiciais, há casos que isso decorre não da desobediência a uma hierarquia jurisdicional ou de desconhecimento técnico da existência de julgados de Cortes superiores em tal

---

[300] Vide: ANDRADE, Daiane. Mesmo com novos peritos, PR ainda tem menos de 50% do efetivo previsto em lei. **Gazeta do Povo**, Curitiba, 23 jul. 2019. Disponível em: https://www.gazetadopovo.com.br/parana/novos-peritos-policia-pr. Acesso em: 3 dez. 2021.

[301] "O exame mais solicitado por todas as instituições é em dispositivos computacionais portáteis principalmente aparelhos de telefonia celular (88%)" (p. 19; Cf.: POLÍCIA CIENTÍFICA DO PARANÁ. **Relatório estatístico 2020**. Disponível em: https://www.policiacientifica.pr.gov.br/Pagina/Relatorio-Estatistico. Acesso em: 20 nov. 2022.

[302] Conforme: PAVANELI, Aline. Demora nas perícias de eletrônicos emperra investigações no Paraná; fila para análise passa de 19 mil aparelhos. **G1**, 18 jul. 2018. Disponível em: https://g1.globo.com/pr/parana/noticia/2018/07/18/demora-nas-pericias-de-eletronicos-emperra-investigacoes-no-parana-fila-para-analise-passa-de-19-mil-aparelhos.ghtml. Acesso em: 2 dez. 2021.

[303] Exemplos de diferentes pontos de vista ficam claros nas audiências públicas da ADI 5527 e ADPF 403 na Suprema Corte, disponíveis no YouTube, resumidas em: COSTA JÚNIOR, Ivan Jezler. **Prova penal digital**: tempo, risco e busca telemática. Florianópolis: Tirant Lo Blanch, 2019, p. 77-81.

[304] Como defendido em: BADARÓ, Gustavo. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. **Boletim IBCCRIM**, São Paulo, v. 29, n. 343, jun. 2021. Disponível em: https://www.ibccrim.org.br/js/pdf-js/web/viewer.html?file=/media/publicacoes/arquivos_pdf/revista-31-05-2021-10-44-29-869137.pdf. Acesso em: 05 dez. 2022.

[305] Vide rodapé n. 154.

sentido, mas do feitio artesanal inerente ao processo-crime, podendo a subsunção do fato à norma variar de acordo com os elementos do caso concreto. Como exemplo, a 6ª Turma do C. STJ já entendeu ser inválida a prova obtida por meio do *print screen* da tela do WhatsApp Web, já que

> é possível, com total liberdade, o envio de novas mensagens e a exclusão de mensagens antigas (registradas antes do emparelhamento) ou recentes (registradas após), tenham elas sido enviadas pelo usuário, tenham elas sido recebidas de algum contato. Eventual exclusão de mensagem enviada (na opção 'Apagar somente para Mim') ou de mensagem recebida (em qualquer caso) não deixa absolutamente nenhum vestígio, seja no aplicativo, seja no computador emparelhado, e, por conseguinte, **não pode jamais ser recuperada para efeitos de prova em processo penal**, tendo em vista que **a própria empresa disponibilizadora do serviço, em razão da tecnologia de encriptação ponta-a-ponta, não armazena em nenhum servidor o conteúdo das conversas dos usuários**" (BRASIL. Superior Tribunal de Justiça. 99.735/SC. Relatora: Min. Laurita Vaz, Sexta Turma, julgado em 27/11/2018. **Diário de Justiça Eletrônico**, Brasília, DF, 12 dez. 2018). [...].[306]

Mas, em recente julgamento, a 5ª Turma do C. STJ, pela prova produzida nos autos e do ônus da prova que não se desincumbiu o acusado, a tese desse julgado acima referido, quanto à invalidez do *print screen* da tela da conversa por WhatsApp como prova no processo, caiu por terra, considerando a motivação do juízo que, no caso, não houve a quebra da cadeia de custódia,

> pois em nenhum momento **foi demonstrado** qualquer indício de adulteração da prova, ou de alteração da ordem cronológica da conversa de WhatsApp obtida através dos prints da tela do aparelho celular da vítima. 3. In casu, o magistrado singular afastou a ocorrência de quaisquer elementos que comprovassem a alteração dos prints, entendendo que mantiveram "uma sequência lógica temporal", com continuidade da conversa, uma vez que "uma mensagem que aparece na parte de baixo de uma tela, aparece também na parte superior da tela seguinte, indicando que, portanto, não são trechos desconexos". 4. O acusado, embora tenha alegado possuir contraprova, quando instado a apresentá-la, furtou-se de entregar o seu aparelho celular ou de exibir os prints que alegava terem sido adulterados, o que só reforça a legitimidade da prova. 5. **"Não se verifica a alegada 'quebra da cadeia de custódia',** pois nenhum elemento veio aos autos a demonstrar que houve adulteração da prova, alteração na ordem cronológica dos diálogos ou mesmo interferência de quem quer que seja, a ponto de invalidar a prova". (HC 574.131/RS. Relator: Ministro Nefi Cordeiro, Sexta Turma, julgado em 25/8/2020, **DJe** 4/9/2020).

De modo muito semelhante a Teoria do Mosaico, após o julgamento da Suprema Corte dos EUA, vem sendo aplicada de forma diversa por todo o território norte-americano, justamente, em face de mudanças fáticas e da tecnologia.

---

[306] BRASIL. Superior Tribunal de Justiça. RHC 133430/PE. AgRg no RHC 133430/PE. Relator: Min. Nefi Cordeiro. **Diário de Justiça Eletrônico**, Brasília, DF, 26 fev. 2021.

Veja-se que das novas tecnologias e a similitude com as questões do direito comparado, há a percepção de mais duas importantes discussões nas Cortes superiores do Brasil para colorir a conclusão supra. Na primeira, decidiu-se que há contaminação do processo por prova ilícita se ausente ordem judicial em caso de autoincriminação forçada[307] pela determinação policial ao acusado de tratar de conversa por viva-voz (STJ, REsp 1630097, rel. Ministro Joel Ilan Paciornik, **Diário de Justiça Eletrônico**, Brasília, DF, 18 abr. 2017). Na segunda, ainda pendente de julgamento em consulta de 21 nov. 2022, já há duas posições antagônicas em votos já proferidos, uma pela licitude da prova, e outros dois pela ilicitude; é o caso da Repercussão Geral no **Tema 977 do STF:** "*Aferição da licitude da prova produzida durante o inquérito policial relativa ao acesso, sem autorização judicial, a registros e informações contidos em aparelho de telefone celular, relacionados à conduta delitiva e hábeis a identificar o agente do crime.*" (BRASIL. Supremo Tribunal Federal. Agravo em Recurso Extraordinário (ARE) 1.042.075. Relator: Min. Dias Toffoli).

Esses julgados espelham situações muito similares aos precedentes norte-americanos tratados no subcapítulo 3.1, na aplicação da Teoria do Mosaico, dadas às vicissitudes do caso concreto. E tais interpretações jurisprudenciais são, naturalmente, divergentes; trata-se de um processo de revelação de premissas prático-teóricas complementares à construção do entendimento judicial.

De todo o exposto, a verdade é que, independente do mérito definitivo dessas futuras ações constitucionais (ADPF 403 e ADI 5527), denota-se a ausência de uma teoria universal aplicável, um conceito único ou último, mas, uma imperativa regulamentação geral normativa, pois o caso concreto pode revelar uma necessidade diversa da tese geral julgada em um precedente[308], além das mudanças tecnológicas inerentes à obsolescência programada ligada, outrossim, à evolução social. Por isso, proeminentes os preceitos das mais diversas origens do direito comparado, a sistematização dos crimes cibernéticos e do direito processual penal por normas

---

[307] Do direito dos EUA, lembre-se que "As duas cláusulas da **4ª** emenda, mais a cláusula do privilégio contra a autoincriminação forçada, da **5ª** emenda, colocam a questão da licitude das provas. Dito em outras palavras, tornam relevante discutir a solução a ser dada à hipótese em que provas foram efetivamente produzidas com infração às garantias veiculadas por essas cláusulas." (RAMOS, *op. cit*, p. 119).

[308] Se há vícios na "documentação da cadeia de custódia, a prova não deve ser necessariamente considerada ilícita, sendo admissível sua produção", motivada a autenticidade e integridade da fonte "para valorar seu conteúdo". (BADARÓ, Gustavo. A cadeia de custódia e sua relevância para a prova penal. In: SIDI, Ricardo; LOPES, Anderson B. (Org.). **Temas atuais da investigação preliminar no processo penal**. Belo Horizonte: D'Plácido, 2018, p. 536.).

específicas voltadas à cooperação internacional probatória entre Estados, a interceptação telefônica e telemática nos aspectos tecnológicos recentes da comunicação digital. E disso não destoa a doutrina:

> Há, contudo, **risco de, diante dos precedentes inflexíveis sobre a exclusão das provas** a partir da má conduta dos policiais, os próprios agentes mentirem sobre a forma de obtenção das provas para driblarem os precedentes das Cortes que, uma vez aplicados, invalidam as provas colhidas. Mais do que isso, pelo pragmatismo inerente ao desenvolvimento das regras de exclusão, se originariamente se visava proteger a privacidade dos cidadãos, **a aplicação casuística acabava por diminuir a proteção porque as Cortes tinham que se debruçar caso a caso sobre a apreciação de violação ou não da privacidade, sem o estabelecimento de regra geral e abstrata**.[309] (Grifo nosso)

Realizado esse incurso inicial para a construção do raciocínio por detrás de todo o imbróglio pesquisado, adentra-se ao tema da interceptação de fluxo de conversas protegidas pela E2EE e as limitações quanto a sua quebra pelas empresas por ordem judicial.

Em síntese, há dois votos favoráveis (cada um nas duas ações distintas, mas que estão sendo julgadas em conjunto: ADPF 403, rel. Min. Edson Fachin, e ADI 5527, de relatoria da Min. Rosa Weber) pela manutenção da criptografia ponta a ponta sem determinação obrigatória de fornecimento de senhas de *backdoor* ou chaves de segurança pelas empresas responsáveis, mesmo diante de ordem judicial para investigação de crimes, e ainda que nos termos da Lei n. 9.296/96. E, atualmente[310], permanecem tais ações pendentes de julgamento, porquanto com vista ao Min. Alexandre de Moraes, que parece ter posicionamento contrário[311] aos aludidos relatores:

> [...] Um grupo de trabalho com juízes, secretários e conselheiros do CNJ propôs uma lista com 11 medidas para melhorar a segurança pública no Brasil. **O coordenador da iniciativa é o ministro Alexandre de Moraes, do STF**, que enviou as propostas para o presidente da Câmara, Rodrigo Maia (DEM-RJ). Elas podem servir de base para as reformas que serão implementadas este ano pelo Congresso e pelo ministro da Justiça, Sérgio

---

[309] VIEIRA, Renato Stanziola. **Controle da prova penal**: obtenção e admissibilidade. São Paulo: Revista dos Tribunais, 2021, p. 67.

[310] Verificação do andamento processual em 21 nov. 2022. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4975500. E ainda: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4983282. Ambos com acesso em: 21 nov. 2022.

[311] Importante ressaltar, portanto, que a posição da Suprema Corte ainda está indefinida. Vide: VENTURA, Felipe. Proposta quer banir WhatsApp e Telegram se não quebrarem sigilo no Brasil. **Tecnoblog**, 9 jan. 2019. Disponível em: https://tecnoblog.net/274333/whatsapp-telegram-quebra-sigilo-proposta-cnj. Acesso em: 21 nov. 2021.

> Moro. **Uma das propostas pede 'meios de acesso e quebra de sigilo de troca de mensagens de membros de organizações criminosas pela internet, redes sociais ou aplicativos de mensagens, inclusive com a possibilidade de infiltração de agentes policiais'. Isso significa que WhatsApp, Telegram, Signal, Facebook Messenger e outros aplicativos deveriam ser obrigados a quebrar o sigilo de mensagens sob ordem judicial. Eles também deveriam oferecer uma forma de grampear pessoas sob investigação. A proposta também diz que esses aplicativos 'deverão ter sede ou representação em território nacional e obrigatoriamente atenderão as determinações que lhes forem dirigidas'**. O WhatsApp, por exemplo, não tem representação oficial no Brasil: qualquer pedido da Justiça precisa ser encaminhado aos EUA, exigindo uma burocracia adicional. [...] (grifo nosso).

Os argumentos dos votos (ADPF 403 e ADI 5527) são expostos, sucintamente, a seguir, mas desde já, evidencia-se que, tal como na evolução jurisprudencial norte-americana, o alcance da interpretação de preceitos constitucionais não está delimitado de forma definitiva, dada a evolução tecnológica constante e eventuais novos dados estatísticos quanto à importância da eventual quebra da criptografia ponta a ponta como pressuposto para, sob o critério da proporcionalidade utilizada como um dos argumentos no voto do ilustre Min. Edson Fachin, preponderar sobre os casos de investigação criminal de delitos graves que resolveria.

O Excelentíssimo Relator da ADPF 403, Min. Edson Fachin, resume as premissas de seu voto, iniciando-se por elencar os direitos digitais como fundamentais; rememora a importância da garantia do direito à privacidade e à liberdade de expressão nas comunicações como condição para o pleno exercício do direito de acesso à internet. Com isso, aduz que a criptografia e o anonimato são especialmente úteis para o desenvolvimento e compartilhamento de opiniões, o que geralmente ocorre por meio de comunicações *online* como o e-mail, mensagens de texto e outras interações; elenca tal proteção por chave de segurança como meio de se assegurar a proteção de direitos essenciais para a vida pública. Sua mais relevante argumentação é no sentido de ser contraditório defender que, em nome da segurança pública, deixe-se de promover e buscar uma internet mais segura, direito de todos e dever do Estado e, neste ponto de vista, sem uma "evidência científica", adotar medidas as quais tragam insegurança aos usuários (como alguma forma de quebra da criptografia ponta a ponta), a qual somente se justifica se houver certeza comparável aos ganhos obtidos em outras áreas, o que não verificou no estudo do caso, doutrina e das manifestações das audiências públicas realizadas.

Por fim, com base em artigos estrangeiros sobre estatísticas até agora conhecidas do uso da criptografia por criminosos, refuta o Exmo. Relator os argumentos da Polícia Federal e do Ministério Público Federal, que pleiteiam pela prevalência do interesse público (segurança pública) sobre o particular (criptografia ponta a ponta por empresas de tecnologia de comunicação, ou seja, privacidade e liberdade de expressão e comunicação). No voto, consigna que, pelas provas produzidas, não há dados concretos, ao menos por ora, de uma escalada significativa no uso da E2EE para o cometimento de crimes graves, e então, neste momento, não há proporcionalidade na vedação de seu uso ou mesmo a permissão de outras maneiras de seu enfraquecimento para a investigação criminal ao se comparar aos demais direitos constitucionais envolvidos, consagrando, porém, a precariedade pela obsolescência programada e a não isenção de alguma responsabilidade (que não implique a quebra da criptografia) das pessoas jurídicas responsáveis pelo serviço de mensageria. Vale colacionar trecho relevante do voto[312]:

> Durante a audiência pública, em pergunta dirigida sobretudo aos representantes dos órgãos de segurança, perguntou-se, especificamente, quais os crimes que exigiriam a investigação preferencialmente ou exclusivamente a partir de interceptações. Os representantes do Ministério Público Federal, mencionaram, especificamente, pornografia infantil, organizações criminosas, tráfico de drogas e tráfico de armas. [...] Em que pesem, porém, os problemas trazidos por quem abusa da liberdade online, **'de acordo com os dados disponíveis, o número de casos afetados pela criptografia é pequeno'**" [...]. No mesmo sentido, David Kaye, no Relatório apresentado ao Conselho de Direitos Humanos, apontou que, não obstante as demandas por acessos especiais à criptografia das empresas de aplicativo, **os Governos ainda não demonstraram que o uso criminoso da criptografia constitui uma barreira insuperável para os objetivos das polícias** [...]. De fato, como restou amplamente demonstrado durante a audiência pública, a concessão de privilégios especiais a agentes do governo para o acesso à criptografia, seja por meio de *backdoors*, seja pela permissão de ataques do tipo *man in the middle*, ou, ainda, pela custódia de chaves (*key escrows*), apresenta riscos graves à segurança de todos. [...] Medidas que, à luz da melhor evidência científica, trazem insegurança aos usuários somente se justificam se houver certeza comparável aos ganhos obtidos em outras áreas. Não é isso, porém, o que ocorre. **O risco causado pelo uso da criptografia ainda não justifica a imposição de soluções que envolvam acesso excepcional**. [...] Em síntese, **é inconstitucional** proibir as pessoas de utilizarem a criptografia ponta-a-ponta, pois uma ordem como essa impacta desproporcionalmente as pessoas mais vulneráveis. É importante frisar, por fim, que **o reconhecimento de um direito constitucional à criptografia forte não diminui nem isenta as empresas que produzem os aplicativos de se conformarem com a legislação brasileira, nem a descumprirem as ordens judiciais que, na medida da estrita proporcionalidade, exijam a entrega de dados que não dependam da quebra de criptografia** [...]. (Grifo nosso).

---

[312] BRASIL. Supremo Tribunal Federal. **ADPF 403/SE**. *Op. cit*, p. 65-71.

Já na ADI 5.527, de relatoria da Excelentíssima Ministra Rosa Weber, sua motivação baseou-se na interpretação dos arts. 7º, II e III; 10, § 2º; 11 e 12, III e IV, todos da Lei n. 12.965/2014 (Marco Civil da Internet). Sintetiza em seu voto fundamentos[313] com supedâneo nas liberdades fundamentais de expressão, de comunicação, da privacidade, o sigilo das comunicações privadas, de nossa Carta Magna (art. 5º, IX, X, XII da CF). Assim decidiu, em destaque:

> (i) julgo improcedente o pedido de declaração de inconstitucionalidade do art. 12, III e IV, da Lei nº 12.965/2014; (ii) julgo procedente o pedido de interpretação conforme a Constituição do art. 10, § 2º, da Lei nº 12.965/2014, a fim de **assentar exegese segundo a qual 'o conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer**, respeitado o disposto nos incisos II e III do art. 7º, **e para fins de investigação criminal ou instrução processual penal'**; (iii) julgo improcedente o pedido sucessivo de declaração de nulidade parcial sem redução de texto do art. 12, III e IV, da Lei nº 12.965/2014, à compreensão de que não abrangido em sua hipótese de incidência o conteúdo que dele se pretende excluir; (iv) julgo parcialmente procedente o pedido sucessivo de interpretação conforme a Constituição do art. 12, III e IV, da Lei nº 12.965/2014 apenas para (a) **assentar que as penalidades de suspensão temporária das atividades e de proibição de exercício das atividades somente podem ser impostas aos provedores de conexão e de aplicações de internet nos casos de descumprimento da legislação brasileira quanto à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como aos direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros**, (b) **ficando afastada qualquer exegese que – isoladamente ou em combinação com o art. 7º, II e III, da Lei nº 12.965/2014 – estenda a sua hipótese de incidência de modo a abarcar o sancionamento de inobservância de ordem judicial de disponibilização de conteúdo de comunicações passíveis de obtenção tão só mediante fragilização deliberada dos mecanismos de proteção da privacidade inscritos na arquitetura da aplicação**. (Grifo nosso).

A julgadora entendeu por existir "lesão à Constituição, diante das ordens judiciais de bloqueio de aplicativos de mensagens", pois "não guarda relação direta com a vigência do Marco Civil da Internet brasileiro, mas com a sua invocação indevida para a prática de atos que não são por ele, Marco Civil, amparados". Enfatizou que a Suprema Corte tem reconhecido que os limites constitucionais do sigilo alcançam as comunicações telemáticas de dados, e, assim, destaca que a inviolabilidade do sigilo das comunicações realizadas pela internet pode ser excepcionada, por ordem judicial (somente), no âmbito da persecução penal "para fins

---

[313] Cf.: BRASIL. Supremo Tribunal Federal. **ADI 5527/DF**. *Op. cit*, p. 35-36.

de investigação criminal ou instrução processual penal". Por fim, da análise de tais dispositivos e da Convenção de Budapeste, concluiu a douta Ministra que

> não pode o Estado compeli-lo a oferecer um serviço menos seguro e vulnerável, sob o pretexto de que pode vir, eventualmente, a utilizar essa vulnerabilidade artificial, para cumprir ordem judicial a respeito. Isso significaria tornar ilegal a criptografia, ou pelo menos alguns de seus usos[314].

Pois bem. Apesar dos fundamentos dos doutos relatores, o exame dos votos evidencia algumas outras conclusões e críticas em face de toda a presente pesquisa científica.

Do voto da douta Ministra Rosa Weber cabe ressaltar que, apesar de, na época, ainda não vigente em nosso ordenamento jurídico a Convenção de Budapeste, esta foi usada em seu voto como *standard* normativo do que se tinha de base futura a ser incorporada, mormente diante dos seus arts. 18 e 21, que tratam no tema da interceptação telemática, mantendo a autonomia dos Estados Parte (Brasil) em legislar previamente sobre os requisitos legais para esse fim, como as infrações penais abrangidas possíveis de tal interceptação, em casos específicos de investigação criminal e processual penal.

Ora, como conclusão prévia, é esta justamente a fórmula legislativa da lei alemã acima referida, objeto deste estudo, apesar das críticas já expostas anteriormente neste trabalho. Outrossim, muito tem a ver com o que dispõe a Lei n. 9296/96. E, como visto, diversamente do que ponderou em seu voto, há sim tendência legislativa e de ações governamentais nos EUA e no Reino Unido, dentre outros países, no sentido de forçar as empresas a criar tecnologia voltada à leitura de mensagens criptografadas, inclusive para a criação de *backdoors*. O ponto controverso, ausente na Lei n. 9296/96, é a determinação da quebra de E2EE pelas empresas privadas, requisito excluído da lei alemã e, cuja interpretação, com fulcro no Marco Civil da Internet, é objeto dessas ações constitucionais em nossa Suprema Corte.

Questão que pode ser objeto de crítica do voto do Exmo. Ministro Edson Fachin é a alusão à estatística em estudo sem base científica oficial (rodapé n. 297).

---

[314] Motiva, ademais, contrariamente ao exposto anteriormente nesta dissertação, que "**A ideia, que não é nova, de forçar a implementação de 'backdoors' (portas dos fundos) em softwares de criptografia, para franquear acesso furtivo a autoridades públicas, ainda que limitada a situações excepcionais, vem sendo abandonada em todo o mundo**. (*Ibid.*, p. 28; grifo nosso).

Da análise das referências que cita em seu voto, nenhuma demonstra ou comprova seguir critérios matemáticos estatísticos, e, não traz dados convincentes em laudo técnico imparcial[315]. Fora isso, tratam de realidades distintas da brasileira[316], com índice de criminalidade que, no mínimo, mereceria a ideia em se pesquisar, cientificamente, o tamanho do impacto nas investigações criminais da possibilidade de interceptação telemática de fluxo de comunicações dotadas de criptografia ponta a ponta em tempo real, ou de imagens, vídeos e outros documentos digitais relevantes para a persecução penal, após a devida ordem judicial. Na Espanha, por exemplo, a doutrina prega uma adaptação da investigação criminal a esta nova era digital, apontando, a figura de uma velada macrovitimização[317], argumento favorável à investigação criminal digital de serviço de mensageria dotada da E2EE, diversamente do voto do douto Min. Fachin, pois as estatísticas citadas em seu voto podem estar mascaradas pelo desconhecido, justamente porquanto objeto de prova impossível, exceto pela escalada na ocorrência de crimes cibernéticos.

Os projetos de lei dos EUA, já comentados neste trabalho, pretendem, ao contrário desses votos, a imposição, mesmo indireta, de quebra de criptografia ponta a ponta, sob pena de responsabilização cível e criminal das empresas que sejam omissas no combate a crimes ligados à pornografia ou exploração sexual de crianças. E isso, repita-se, repercute na dificuldade da conciliação de todo o arcabouço jurídico internacional para a efetivação da pretendida cooperação jurídica internacional através da Convenção de Budapeste, até porque, prevalecendo tais entendimentos no STF, irá de encontro ao núcleo legislativo vigente da Alemanha (permitindo a interceptação telemática de mensagens com a E2EE por "cavalo de Troia" do Estado) e os projetos de lei do Reino Unido e dos EUA.

---

[315] Dados das companhias traz o aumento nos requerimentos de dados **"de até 535% entre os anos de 2015 e 2020**" (FONTENLA, Carolina Paulino. Desafios da cooperação entre empresas de internet e Poder Público. **Migalhas**, 9 jun. 2021. Disponível em: https://www.migalhas.com.br/depeso/346738/desafios-da-cooperacao-entre-empresas-de-internet-e-poder-publico. Acesso em 22 jun. 2021).

[316] Em 2017 o Brasil foi o "segundo país com maior número de casos de crimes cibernéticos, afetando cerca de 62 milhões de pessoas e [...] prejuízo de US$ 22 bilhões". Vide: UOL. **Brasil é o segundo país no mundo com maior número de crimes cibernéticos**. São Paulo, 15 set. 2018. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2018/02/15/brasil-e-o-segundo-pais-no-mundo-com-maior-numero-de-crimes-ciberneticos.htm. Acesso em: 22 jun. 2021.

[317] "[...] devemos apontar que muitos desses delitos não são descobertos, são descobertos tarde ou por puro azar. Nesse sentido, existe uma macro-vitimização muito difícil de determinar ou quantificar", cf.: ANDRÉS, Moisés Barrio. **Ciberdelitos Amenazas criminales del ciberespacio**. Madrid: Reus, 2017, p. 49; grifo e tradução nossos).

Aliás, dentre as

> tendências mais preocupantes deste debate é o caráter estritamente doméstico da implementação das regulações, quando formalizadas. Ainda que diversos países estejam debatendo concomitantemente as mesmas questões apresentadas, as soluções apresentadas tomam a forma de políticas nacionais de regulação, **sem a preocupação de possíveis efeitos que podem gerar além das fronteiras jurisdicionais do Estado regulador, impactando em outras regulações nacionais e na integridade do sistema criptográfico em nível global**. (Grifo nosso). [318]

Importante ressaltar o óbvio interesse negocial das empresas de tecnologia em manter a criptografia ponta a ponta, como a recente transação bancária por meio do WhatsApp, ou, manter sua clientela na busca de uma comunicação absolutamente sigilosa. Mas, como ressalta a doutrina, é

> ônus do parecerista ou consultor ser uma fonte confiável. Para tanto, o primeiro aspecto que precisa ser por ele observado é a sua independência e falta de interesse negocial ou no deslinde da causa sobre a qual está sendo consultado. [319]

Assim, obviamente que, durante as audiências públicas na Suprema Corte brasileira e manifestações na imprensa por todo o mundo, a defesa de tais empresas é pela manutenção da criptografia ponta a ponta.

Veja-se que a questão da responsabilidade civil e criminal das empresas responsáveis pelas mensagens transmitidas e seus conteúdos é outro ponto controvertido, mas que já se debruçou a jurisprudência e o legislador (arts. 18 e 19 do Marco Civil da Internet) em casos análogos[320], e, contrariamente ao objetivo do Projeto de lei norte-americano denominado "EARN IT Act", o sentido que se sinaliza é o de afastar a responsabilidade objetiva (exceto em relações de consumo) dessas companhias, para o cabimento tão só da subsidiária e subjetiva em caso de "desídia a uma ordem judicial competente", argumento que, em certa medida, o STF está se debruçando nessas ações constitucionais, mormente visando à efetividade da decisão final dos Acórdãos, pois, a criptografia ponta a ponta, por si só, ou seja, afastadas hipóteses excepcionais de meios alternativos de investigação, é inviolável.

---

[318] Cf.: DONEDA, Danilo; MACHADO, Diego (Org.). **A criptografia no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2020, RB-3.1. E-book, posições 2441 e 2451.

[319] Ver: CARUSO, Tiago. **Responsabilidade penal nas decisões embasadas em pareceres técnicos e jurídicos**. São Paulo: Marcial Pons, 2020, p. 187.

[320] MAGRO, Américo Ribeiro; ANDRADE, Landolfo. **Manual de direito digital**. São Paulo: Juspodivm, 2021, p. 261.

O problema a ser resolvido é até que medida essas empresas estão disponíveis a cooperar com o Estado[321], já que os princípios que se almejam resguardar são todos legitimamente defensáveis. É um novo paradigma estabelecido, chamado pela doutrina de "modelo da proceduralização" [322], com fulcro em constitucionalistas da Alemanha:

> Especialmente em âmbitos complexos como os das novas tecnologias, o conhecimento necessário para a tomada da decisão não se encontra no Estado, tornando assim necessária a criação de novas formas de geração do conhecimento dentro do direito regulatório estatal que incorpore o conhecimento advindo da sociedade. [...]
> Enquanto o modelo da ponderação incorpora em seu modelo um horizonte reduzido de formulação de novas distinções e conceitos jurídicos para orientar novas decisões, ficando a cabo de um situacionismo do caso a caso, o modelo da proceduralização foca na dimensão processual para aquisição de conhecimento para decisão em âmbitos complexos da sociedade na qual **o conhecimento para decisão não decorre de uma simples ponderação de dois princípios abstratos.**
> [...]
> Essa forma de regulação se foca essencialmente na **cooperação entre o Estado regulador e os atores ou setores sociais a serem regulados**. No contexto da sociedade das plataformas essa seria uma importante maneira de regulação mais condizente com a nova complexidade social. (Grifo nosso)

Relembre-se, destarte, a advertência doutrinária sobre o perigo dos precedentes inflexíveis para evitar a exclusão de provas relevantes, a necessidade de uma lei formal, geral e abstrata, quanto ao controle epistêmico na produção e admissibilidade da prova digital penal e o estudo do direito comparado como algo indissociável ao novo rumo do devido direito processual penal. A soma do desenvolvimento das novas tecnologias e a sociedade da plataforma moldam de forma diversa o futuro da sociedade e do Direito, "caracterizada por uma participação mais ampla de múltiplos atores nessa modelagem".[323]

O estudo individualizado da Convenção de Budapeste, portanto, é o próximo passo para a completa exposição do arcabouço jurídico vigente no Brasil.

---

[321] As *Big Techs* têm requerido a "colaboração de instituições encarregadas de vigiar a verossimilhança" contra informações falsas, num processo de "auto-regulamentação" (p. 270; tradução nossa – Cf.: RICCI, Sergio Diaz. El derecho a la privacidade en la era digital: uma experiência comparada. In: CÉSAR, Joaquim; MEZZETTI, Luca. (Org.). **O direito das novas tecnologias e o ordenamento constitucional**. Belo Horizonte: D'Plácido, 2021).

[322] ABBOUD, Georges; CAMPOS, Ricardo. A autorregulação regulada como modelo do Direito proceduralizado. In: ABBOUD, Georges; NERY JR., Nelson; CAMPOS, Ricardo (Org.). **Fake News e Regulação**. 3. ed. São Paulo: Thomson Reuters Brasil, 2021, p. 143-144.

[323] CAMPOS, Ricardo. **Metamorfoses do direito global: sobre a interação entre Direito, tempo e tecnologia.** São Paulo: Contracorrente, 2022, p. 330.

4.3 A CONVENÇÃO DE BUDAPESTE E SUAS INTERCORRÊNCIAS À PRODUÇÃO DA PROVA PENAL DIGITAL

A necessidade de um tratado internacional sobre a persecução penal, tal como a Convenção de Budapeste (também chamada de Convenção do Conselho da Europa contra a Criminalidade Cibernética[324]), adequando-se ao ordenamento jurídico de cada Estado participante, advém da procura em evitar a produção de prova ilícita e agilizar os atos de cooperação internacional[325] na interceptação telefônica ou telemática de fluxo de dados por aplicativos de mensagens via internet[326], resultando no combate mais célere de crimes graves. Além disso, resulta no natural incremento, pela troca e manejo de experiências estrangeiras, de novos entendimentos jurisprudenciais, textos normativos e da própria tecnologia mais eficiente à materialização das investigações penais digitais para eventuais adaptações em cada Nação.

Apesar do novo tratado internacional, permanece a árdua implementação prática, no Brasil, do fim perquirido pela Convenção de Budapeste, daí o necessário incurso neste subcapítulo por diversas nuances. Uma delas, será o exame de entendimentos do STF sobre a cooperação jurídica internacional em matéria probatória penal, em especial a digital; e, a outra, de legislação norte-americana como pesquisa comparativa, mormente por sua influência digital e socioeconômica (país sede das *Big Techs*), tal qual exposto no capítulo 2.

Ao se propor uma cooperação jurídica internacional em matéria de provas penais os desafios não são poucos, como visto nas diferentes formas de intervenção do Estado, postas e propostas, na produção daquelas dotadas de criptografia ponta a ponta nos EUA, Reino Unido e Alemanha. Mas é possível:

---

[324] A Convenção de Budapeste [...] resta aderida por 62 Estados Partes, com 10 países observadores, incluindo os Estados Unidos, a Rússia e alguns países da América Latina**"**. Cf.: CONSELHO DA EUROPA. **Convenção sobre o Cibercrime**. Budapeste, 23 nov. 2001. Disponível em: https://rm.coe.int/16802fa428. Acesso em: 18 nov. 2021.

[325] Tida como uma "referência mundial" (ZANIOLO, Pedro Augusto. **Crimes modernos**: o impacto da tecnologia do direito. 4. ed. Salvador: JusPodivm, 2021, p. 665).

[326] Há previsão das formas e limites de obtenção de dados de tráfego e de conteúdo em tempo real de dados informáticos nos arts. 20 e 21 da Convenção de Budapeste, em ambos, **limitando a responsabilidade da empresa à possibilidade técnica da interceptação.**

> Os ordenamentos jurídicos estatais, conectados por exigência de repressão internacional aos delitos (cooperação jurídico-penal internacional) e por critérios de justiça consagrados em tratados de direitos humanos, configuram sistemas similares entre si de controle epistêmico das atividades probatórias, com independência de tratar-se da tradição do Common Law ou do direito continental europeu a que nos filiamos.[327]

Para se ter ideia da complexidade do tema, hipótese que é pacificamente aceita como prova do ponto de vista do sistema interno de um país, num primeiro olhar bitolado voltado ao seu ordenamento jurídico, pode contemplar divergência noutro país que se pretenda auxílio na produção da prova penal. Exemplo disso: a serendipidade. Extremamente usual de ocorrência na investigação criminal e admitida por lei e jurisprudência aqui no Brasil, não nos parece que seja diferente noutros países. Ledo engano. Ilustra-se isso a partir de lição doutrinária que discorre sobre os conhecimentos fortuitos ou ocasionais daqueles originários do crime que se almeja, inicialmente, investigar, prova inadmissível (via de regra) no direito italiano e alemão, destoando do brasileiro[328]:

> **No direito comparado, há entendimentos diversos:** [...] Segundo o § 100.b.5, da *StPO*, as informações pessoais obtidas pelas medidas referidas na oitava seção (confisco, interceptação telefônica, *v.g.*) somente podem ser utilizadas como prova em outros procedimentos na medida em que originárias de conhecimentos necessários ao esclarecimento dos crimes referidos na letra anterior, ou seja, expressamente catalogados (homicídio, roubo, extorsão, alta traição, *v.g.*). [...] O art. 270.1 do CPP italiano prevê que os resultados das interceptações telefônicas não podem ser utilizados em procedimentos diversos daqueles nos quais foram autorizados, salvo quando resultarem indispensáveis à prova de delitos em que o flagrante seja obrigatório.[329]

Veja-se, todavia, que a professora Dra. Teresa Armenta Deu, ao realizar denso estudo do direito comparado de diversas Nações (Reino Unido, Alemanha, Portugal, França, EUA, Brasil etc.) sobre a prova ilícita voltada à persecução penal no sistema anglo-americano e europeu continental, sintetiza essa divergência normativa como natural, pois

> não existe um tratamento perfeito, no modo e nem no tempo, nem provavelmente com vocação universal, para todos os casos. Ademais, qualquer discussão jurídica será induvidosamente parcial e imperfeita, e será

---

[327] PRADO, Geraldo. **A cadeia de custódia da prova no processo penal**. 2. ed. São Paulo: Marcial Pons, 2021, p. 192.
[328] Vide rodapé n. 391.
[329] Cf.: GIACOMOLLI, Nereu José. **O devido Processo Penal**: abordagem conforme a Constituição Federal e o Pacto de São José da Costa Rica. São Paulo: Atlas, 2014, p. 176.

> influenciada, entre outros aspectos, pela tremenda permeabilidade da doutrina sobre a prova ilícita e às idas e vindas em matéria de segurança pública ou às importantes reações pendulares ante a percepção de um aparente hipergarantismo e a reação contrária frente à impunidade, pouco explicáveis à opinião pública, articulando o devido equilíbrio entre as garantias. Esta realidade, sem embargo, não deve impedir a fixação de regras mínimas [...]. [330]

Logo, no final, o relevante é a segurança jurídica, a taxatividade ("regras mínimas"), algo já pacificado nas diversas Nações democráticas, ainda que com divergências, como necessário ao devido processo legal na produção probatória penal, daí a relevância da Convenção de Budapeste. Essa taxatividade, aliás, não é tratada de forma diversa quanto à E2EE em todos os países verificados neste estudo.

Em vista disso, inerente o exame mais aprofundado da Convenção de Budapeste e do que circunda sua aplicação, ainda que de base normativa generalista, inerente à conjugação de esforços para sua possível internalização no ordenamento jurídico dos países signatários.

Do ponto de vista do direito material, o Brasil desde algum tempo já verificou a necessidade de tutelar novos bens jurídicos penalmente relevantes ao "sistema informático": os crimes cibernéticos (divididos por parte da doutrina como "próprios e impróprios"). Parte do relatório inicial do Projeto do novo Código Penal sintetiza essa **classificação de crimes cibernéticos** e sua conexão aos ditames da Convenção de Budapeste:

> **a) dos crimes cibernéticos impróprios –** praticados com a utilização de sistema informático: o bem da vida a ser preservado será o correspondente a cada uma das condutas ilícitas cometidas; somente apresenta-se um novo "modus operandi", [...]. **b) dos crimes cibernéticos próprios –** relacionados diretamente com o sistema informático: protege-se em linhas gerais a confidencialidade – os dados informáticos só estarão disponíveis para pessoas previamente autorizadas pelo sistema informático; a integridade – a segurança de que o documento eletrônico e os dados informáticos não foram de qualquer forma manipulados, sendo no todo ou em parte destruídos ou corrompidos; e a disponibilidade – o funcionamento e o tratamento do sistema informático (armazenamento, recuperação, transmissão) devem ser efetivos. Nesse sentido, **o Novo Código Penal, em observância ao princípio constitucional da legalidade, deverá tipificar de forma autônoma novas condutas ilícitas relacionadas com o sistema informático**: crime de intrusão e crime de sabotagem informática. Essa tutela dos crimes cibernéticos refere-se a um **novo bem jurídico**, qual seja, **o sistema informático.** [...] Pretende-se harmonizar as termologias adotadas com as utilizadas na **"Convenção de Budapeste sobre Cibercrime**", a fim de introduzir conceitos legais para regular os aspectos da "Sociedade da

---

[330] DEU, Teresa Armenta. **A prova ilícita**: um estudo comparado. Tradução: Nereu José Giacomolli. São Paulo: Marcial Pons, 2014, p. 180.

> Informação" como **técnica legislativa adequada** que avança sobre matérias específicas de outras ciências. [331] (Grifo nosso).

E tal constatação é corroborada pelas diversas reformas em tipos penais já existentes e outros novos que foram introduzidos em nosso país[332], sem dizer do Projeto do novo Código Penal[333] tratá-los em Título próprio (arts. 208 a 211), tipificando os crimes de intrusão (art. 209) e de sabotagem informática (art. 210).

Para a efetividade da investigação de crimes cibernéticos, portanto, deve-se ter um novo olhar ao Direito Penal[334], mas não somente. É que ponto fundamental de sua completude é o direito processual penal[335], além da demonstração evidente da imprescindível cooperação jurídica internacional em matéria de produção de provas penais digitais, já que os crimes cibernéticos costumam ultrapassar as fronteiras:

> Mesmo que a conduta delitiva não atinja outros Estados ou não produza efeitos para além do território nacional, **é comum que seja necessário buscar uma prova no exterior, diante do fenômeno da "internacionalização das evidências",** seja em razão da movimentação das pessoas, da porosidade das fronteiras e também o **amplo acesso à internet**. Se há duas décadas era possível a um agente de persecução fazer seu trabalho sem se valer do auxílio de outros Estados, **atualmente a realidade é completamente diferente**.[336]

De fato, dá-se uma indissociável combinação do direito penal e processual penal, tanto que ambos são abrangidos na Convenção de Budapeste. Veja-se que se o bem jurídico penalmente relevante não for tutelado no país onde se produziu a prova (dupla tipificação), a cooperação entre os órgãos competentes, em diversas ocasiões,

---

[331] Cf.: SILVA, Marco Antonio Marques da. Relatório Final do Anteprojeto do Código Penal. **Senado Federal**, Brasília, DF, 12 jun. 2012. Disponível em: https://www.mpma.mp.br/arquivos/CAOPCRIM/Relat%C3%B3rio%20final%20do%20Anteprojeto%20do%20Novo%20C%C3%B3digo%20Penal.pdf. Acesso em: 13 jun. 2021.

[332] No Brasil, os mais recentes citados no rodapé n. 299.

[333] BRASIL. Senado Federal. Projeto de Lei n. 236, de 2012. **Diário do Senado Federal**, Brasília, DF, 10 jul. 2012. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=3515262&ts=1613697834640&disposition=inline. Acesso em: 13 jun. 2021.

[334] Cf.: BITENCOURT, Cezar Roberto. **Código Penal Comentado**. 8. ed. São Paulo: Saraiva, 2014, p. 678: "Tem havido, em todo o mundo, a criação de novos crimes cibernéticos, decorrentes da necessidade de ordenar, disciplinar e limitar o uso indevido da moderna e avançada tecnologia cibernética".

[335] A doutrina alemã evidencia essa conclusão: "[...] a maioria dos especialistas está de acordo que a parte processual de como investigar e ajuizar eficazmente os cibercrimes exige mais atenção legislativa (e da acusação) que o direito penal substantivo" (Em: BRODOWSKI, Dominik. **Cibercrimen y Protección de la Seguridad Informática**. Tradução: María Belén Linares. Buenos Aires: Ad-Hoc, 2021, p. 106; grifo e tradução nossos).

[336] CF.: MENDONÇA, Andrey Borges de. **Cooperação Internacional**... *Op. cit*, pp.30-31, grifo nosso.

poderá ficar prejudicada[337], a depender do caso[338]. Porém, restou viabilizada na Convenção de Budapeste a cooperação entre os Estados Parte através da flexibilização do princípio da dupla incriminação: no seu art. 25, item 5, impõe-se tão só uma equivalência dos elementos do tipo dos países requerente e requerido, não importando o nome exato do tipo penal, mas a conduta prevista, a subsunção do fato à norma[339].

No denominado Estado Constitucional Cooperativo, admitido na Constituição Federal brasileira[340], defende-se, dada a necessidade inerente ao enfrentamento de uma crise quanto à capacidade de combater a criminalidade cibernética e à produção de provas digitais oriundas de todo o globo, a redução da soberania, mas com um escopo positivo à concretização do resguardo de direitos e garantias fundamentais não só da vítima, mas do próprio acusado:

> **Produz-se uma crise do Estado, pois se percebe a impossibilidade de os países enfrentarem, de maneira local, problemas que são globais** – entre eles a proliferação da criminalidade transnacional e a criminalidade de massa. **Os Estados não podem enfrentá-los, de maneira adequada, isoladamente, nem os princípios tradicionais de jurisdição dão respostas adequadas.** Isso se reflete, de maneira mais ampla, na própria função e no papel que o Estado deve desenvolver, e, de maneira mais específica, na **necessidade de refundar e repensar os aspectos tradicionais da persecução penal**, ainda limitada aos espaços internos de cada país e fundada no princípio da territorialidade.[341]

---

[337] Essa "dupla incriminação" possui 3 hipóteses nos tratados de cooperação jurídica internacional de que o Brasil faz parte: "(i) mantêm-no para toda e qualquer cooperação; (ii) limitam-no a pedidos de cooperação que impliquem medidas coercitivas; e (iii) afastam-no expressamente." Cf.: BELOTTO, Ana M. de S.; MADRUGA, Antenor; TOSI, Mariana T. Dupla incriminação na cooperação jurídica internacional. **Boletim IBCCRIM**, São Paulo, v. 20, n. 237, p. 15-16, ago. 2012.

[338] Frise-se que no caso de extradição, apesar do princípio da dupla tipicidade no exame do pedido pelo STF, há a "pré-exclusão de qualquer debate judicial em torno do contexto probatório [...]." In: BRASIL. Supremo Tribunal Federal. Extradição n. 669. Relator: Min. Celso de Mello. Julgamento em 6 de março de 1996. **DJ**, 29 mar. 1996.

[339] Neste sentido: DELGADO, Vladimir Chaves. **Cooperação Internacional em matéria penal na Convenção sobre o Cibercrime**. 2007. 315 f. Dissertação (Mestrado em Direito das Relações Internacionais) – Centro Universitário de Brasília, 2007, p. 232. Disponível em: https://repositorio.uniceub.br/jspui/bitstream/123456789/3562/3/vladimir.pdf. Acesso em: 22 nov. 2022.

[340] In: MENDONÇA, Andrey Borges de. **Cooperação Internacional no Processo Penal**: a transferência de processos. São Paulo: Thomson Reuters, 2021; p. 51.

[341] *Ibid.*, p. 35, grifo nosso.

Não por acaso que a Convenção de Budapeste dispõe[342] que se estabeleça, no direito interno de cada Estado Parte, a criação, por lei, de diversos tipos penais[343] para a sua devida implementação, abrangendo a tentativa, coautoria e a responsabilidade penal da pessoa jurídica[344].

Cabe advertir, todavia, que não podemos ser inocentes em questões que afetam a soberania dos Estados-parte dessa convenção internacional, por conta de seus interesses econômicos e políticos, pois

> Diante da inexistência de uma estrutura de poder superior da qual provenha claramente a matriz interpretativa de uma norma, e levando em conta que os intérpretes vêm de experiências diversas (formadas por caracteres sociais, políticos e ideológicos peculiares à sua experiência), o texto da norma cede à interpretação soberana. Daí uma reconhecível **esquizofrenia no Direito Internacional, identificada em um amplo espectro de casos, especialmente em questões mais delicadas e politizadas, tais como a "segurança internacional" e o "uso da força."** [345] (Grifo nosso).

A fim de complementar esta integração mundial no combate aos crimes cometidos pela internet e a cooperação em matéria probatória criminal, interessante pontuar que tramita na Câmara dos Deputados o Projeto de lei n. 4.939/2020[346], o qual estabelece princípios e diretrizes à aplicabilidade do Direito da Tecnologia da Informação, além de normas de obtenção e admissibilidade de provas digitais na investigação e no processo; define crimes e penas (art. 1º), mantendo a interceptação telemática de dados em transmissão como um dos meios de obtenção da prova digital

---

[342] Ilustre-se: "Capítulo II – Medidas a tomar a nível nacional; Seção 1 – Direito penal material; Título 1 – Infrações contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos; Título 2 – Infrações relacionadas com computadores; Título 3 – Infrações relacionadas com o conteúdo; Título 4 – Infrações relacionadas com a violação do direito de autor e direitos conexos."

[343] Como os artigos: 2º – Acesso ilegítimo; 3º – Interceptação ilegítima; 4º – Interferência em dados; 5º – Interferência em sistemas; 6º – Uso abusivo de dispositivos; 7º – Falsidade informática; 8º – Burla informática; 9º – Infrações relacionadas com pornografia infantil; 10 – Infrações relacionadas com a violação do direito de autor e dos direitos conexos; 11 – Tentativa e cumplicidade; 12 – Responsabilidade de pessoas "coletivas".

[344] Enfatizando parte da doutrina que "a responsabilidade penal da pessoa jurídica é instrumento de redução da seletividade sistêmica, vez que viabiliza um tratamento igualitário – ao menos no âmbito de criminalização primária [...]". In: PONTAROLLI, André Luis. Política criminal e responsabilidade penal da pessoa jurídica. **Justiça e Sistema Criminal**, Curitiba, v. 10, n. 18, jan./jun. 2018, p. 112.

[345] DISSENHA, Rui Carlo. Cooperação jurisdicional penal internacional: o difícil conflito entre os planos jurídico e político na justiça penal. In: SOUZA, André Peixoto de (Org.). **Estado, poder e jurisdição**. Rio de Janeiro: GZ, 2015, p. 136.

[346] Está presente na justificativa do parlamentar proponente diversas legislações em que se baseia tal projeto legislativo, dentre elas, a Convenção de Budapeste. BRASIL. Projeto de Lei n. 4.939/2020. Autor: Hugo Leal. **Câmara dos Deputados**, Brasília, DF, 15 out. 2020. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1936366&filename=PL+4939/2020. Acesso em: 6 jul. 2022.

na seara criminal (art. 9º, III; art. 10) e a infiltração virtual (arts. 26 a 29), enfatizada a seriedade da cooperação jurídica internacional (art. 2º, IV). Dispõe sobre diversos tipos penais[347], que abrangem os previstos na Convenção de Budapeste, possibilitando sua aplicação em nosso ordenamento jurídico.

Semelhante a tal projeto legislativo, e, inerente à tentativa global de uma maior eficiência na cooperação jurídica internacional na questão probatória penal digital, é a *Cloud Act*, lei norte-americana vigente desde 2018

> para acelerar o acesso a informações eletrônicas mantidas por provedores globais baseados nos EUA [...] para as investigações de [...] parceiros estrangeiros sobre crimes graves, desde terrorismo e crimes violentos exploração sexual de crianças e crimes cibernéticos.[348]

e tais países seriam aqueles tidos por possuírem proteções robustas para "privacidade e liberdades civis".[349]

O *Cloud Act* é expresso à aplicabilidade do *Stored Communications Act* para os dados mantidos no exterior por empresas estabelecidas no território dos EUA (mesmo se estiverem os dados armazenados fora do território norte-americano), e, cria a possibilidade de acordos executivos que permitiriam a comunicação direta de solicitações de dados entre os EUA e outros países, em uma via de mão dupla sob crítica doutrinária, pois

> todas as empresas submetidas ao SCA, ao receberem uma ordem judicial ou um pedido de fornecimento de dados de uma autoridade de governo com quem os EUA mantenham um acordo executivo, estarão autorizadas a fornecer os dados solicitados sem que isso implique em uma violação do SCA, como acontecia anteriormente.[350]

E, no Brasil, o STF segue esta ideia de facilitação, ou, de desburocratização da colheita da prova, inclusive daquelas produzidas em casos criminais de interceptação telemática por tratado internacional bilateral:

---

[347] São os crimes de: Falsidade informática (art. 31); Dano informático (art. 32); Sabotagem informática (art. 33); Acesso ilícito (art. 34); Interceptação ilícita (art. 35); revogando-se (art. 37), pois ora disciplinados, os já vigentes artigos 154-A e 313-A, ambos do Código Penal.

[348] In: GUIDI, Guilherme Berti de Campos. O Cloud Act e os reflexos na sistemática de produção de provas no estrangeiro. **Revista de Direito e as Novas Tecnologias**, São Paulo, v. 3, abr./jun. 2019. 3. Disponível em: https://bd.tjdft.jus.br/jspui/handle/tjdft/49610. Acesso em: 24 nov. 2022.

[349] Cf: UNITED STATES OF AMERICA. Departamento da Justiça. **Cloud Act Resources**. Disponível em: https://www.justice.gov/criminal-oia/cloud-act-resources. Acesso em: 24 nov. 2022.

[350] GUIDI... *Op. cit*, p. 9.

> [...] 3. Não se vê, no caso em tela, ofensa às disposições do Tratado de Assistência Mútua em Matéria Penal celebrado entre o Governo da República Federativa do Brasil e o Governo do Canadá — internalizado pelo Decreto 6.747/2009 -, porquanto **as mensagens interceptadas foram trocadas em território brasileiro e por pessoas com residência no Brasil, sendo a interceptação, inclusive, deferida por autoridade judicial brasileira.** Ressalte-se que uma das finalidades fundamentais dos tratados de cooperação jurídica em matéria penal é justamente **"a desburocratização da colheita da prova"** (MS 33.751, de minha relatoria, Primeira Turma, **DJe** de 31.3.2016), de modo que, cumpridas as exigências legais do direito interno brasileiro, **eventual inobservância a formalidades previstas no acordo internacional não acarretaria a ilicitude da prova**.[351] (Grifo nosso)

Aliás, enfrenta nossa Suprema Corte, na ADC 51 (com vista ao Min. Alexandre de Moraes[352]) fato semelhante ao disposto no *Cloud Act*[353]. O caso refere-se à cooperação jurídica internacional, e, ao dever de as empresas de tecnologia insculpido no art. 11 do MCI[354] e no art. 18 da Convenção de Budapeste[355]. O relator, Min. Gilmar Mendes, proferiu voto para declarar a constitucionalidade dos dispositivos indicados, sem prejuízo da possibilidade de solicitação, diretamente, de dados e comunicações eletrônicas das autoridades nacionais a empresas de tecnologia, conforme as hipóteses desses dois dispositivos legais, com comunicação desta decisão aos Poderes Legislativo e Executivo brasileiros para sua efetividade material; foi acompanhado, por ora, no mérito, por mais dois Ministros: Nunes Marques e André Mendonça. Para o douto Min. Relator,

> [...] o único instrumento cabível para a solicitação de dados eletrônicos é o da cooperação prevista pelo tratado bilateral [MLAT[356]] e as cartas rogatórias. Porém, Mendes também considerou possível que as autoridades brasileiras solicitem essas informações diretamente às empresas localizadas no exterior para as atividades de coleta e tratamento de dados que estejam sob a posse ou o controle de empresa com representação no Brasil e para os crimes cometidos por pessoas localizadas em território nacional. Segundo o relator, essas hipóteses estão contidas no artigo 11 do Marco Civil da Internet, que encontra respaldo no artigo 18 da Convenção de Budapeste.[357]

---

[351] STF, 2ª Turma, Inquérito 3.990/DF. Relator: Min. Edson Fachin. Julgado em: 14 mar. 2017. **DJe**, 02 jun. 2017.

[352] BRASIL. Supremo Tribunal Federal. **ADC 51**. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5320379. Acesso em: 24 nov. 2022.

[353] E são muito semelhantes aos casos reportados no subcapítulo 2.3, especialmente o voto divergente em julgado norte-americano de rodapé n. 73.

[354] Vide nota de rodapé n. 294.

[355] De título nominado como "Ordem de exibição".

[356] É o Acordo de Assistência Judiciária em Matéria Penal (MLAT, na sigla em inglês) celebrado entre o Brasil e os EUA (Decreto Federal n. 3.810/01), que trata da obtenção de conteúdo de comunicação privada sob controle de provedores de aplicativos de internet sediados fora do país.

[357] In: BRASIL. Supremo Tribunal Federal. **Gilmar Mendes vota pela possibilidade de solicitação de dados diretamente a provedores no exterior.** Disponível em:

E complementa o Min. Nunes Marques, em seu voto favorável à regra do art. 11 do MCI, que

> os arquivos eletrônicos não são exatamente objetos transportados fisicamente de um lugar para o outro.[358] [...] Não faz sentido tratá-los como coisas com pesos e dimensões, que precisem de alguma autoridade no exterior para serem trasladadas até aqui[359]

Enfim, após este necessário incurso do cenário brasileiro e internacional do que já se vem debatendo nas Cortes e por legislação voltada à cooperação jurídica internacional, volta-se à Convenção de Budapeste em si, como esperança de maior efetividade em matéria probatória penal, mas, como acima visto, dotado de diversas intercorrências até o assentamento de uma unicidade prática, dado o intricado arcabouço jurídico em seu entorno.

De qualquer maneira, sua recente introdução no ordenamento jurídico brasileiro deve ser comemorada, tendo a proteção dos dados como um direito fundamental. As vítimas de crimes cibernéticos, sem seus regramentos normativos penais e processuais penais, ficariam mais uma vez alijadas de proteção jurídica, sem contar sérios casos de defesa nacional. Aliás, da leitura dos novos tipos penais do ordenamento jurídico brasileiro não se verifica um Direito Penal meramente simbólico, mas necessário nos dias atuais[360], alicerçado agora pela adequação aos ditames de reciprocidade da Convenção de Budapeste.

Porém, deve-se alertar de certas intenções maliciosas na criação de tipos penais usados com clara face de se obstarem direitos consagrados dos cidadãos, utilizando-se da vítima como atração midiática e política[361], como parece ser no caso

---

https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=495011&ori=1. Acesso em: 24 nov. 2022.

[358] Tal como já se criticou julgado norte-americano, nos termos do referido rodapé n. 73.

[359] *Idem*. **Pedido de vista adia julgamento sobre obtenção de dados de provedores de internet no exterior.** Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=495363&ori=1. Acesso em: 24 nov. 2022.

[360] Cf.: BUSATO, Paulo César. **Direito penal**: parte especial. 2. ed. São Paulo: Atlas, 2016. v. 1, p. 401-402: "A importância crescente do armazenamento de dados e informações, a dependência da organização pública e privada em relação ao bom funcionamento dos sistemas de computadores, o volume de informações armazenadas por provedores, compelem a **reconhecer a existência de algo mais em termos de valores, sobre o que deve debruçar-se o legislador**" (grifo nosso).

[361] "Assim, uma utilização política e midiática das vítimas em alguns casos e, em outros, o abuso do estatuto da vítima, perturbam gravemente nosso modelo constitucional e resgatam o arcaico paradigma da "vingança privada", como eixo do Direito Penal" (cf.: GONZÁLEZ CUSSAC, José Luis;

norte-americano e do Reino Unido dos projetos de lei para, veladamente, acabar com a criptografia ponta a ponta, utilizando-se da pedofilia e da pornografia infantil como pano de fundo. A discussão e o levantamento de argumentos a favor e contra tal regra de segurança por sistema de E2EE são relevantes, contudo, não é essa a constitucional e científica maneira de agir, mas de uma integração democrática[362] para sua efetividade por convencimento válido por países das mais diversas linguagens[363], abrangendo fundamentos constitucionais e sistemas jurídicos distintos[364], para resumir.

Tenha-se em mente que os bens jurídicos informáticos, uma vez tutelados pelo direito penal, não possuem qualquer garantia efetiva de que não serão violados ou postos em perigo, compondo mero "elemento justificante da intervenção penal".[365]

Pode-se resumir haver intrínseca interlocução do direito penal e processual penal na eficaz tutela dos bens jurídicos protegidos quanto aos crimes cibernéticos, constatação que, apesar de antes já existente, agora é superlativa pela difícil produção de provas digitais nesta nova era tecnológica, notadamente pela E2EE, a diminuta colaboração das empresas de tecnologia, a adaptação legislativa no direito interno e internacional, além da falta de estrutura policial, sem contar os posicionamentos jurisprudenciais naturalmente atrasados em relação aos fatos que já deviam estar abarcados pelo arcabouço jurídico-normativo.

BUSATO, Paulo César; CABRAL, Rodrigo Leite Ferreira. **Compêndio de Direito Penal Brasileiro**: parte geral. Valencia: Tirant lo blanch, 2017, p. 289-290).

[362] Tem-se utilizado do termo "ciberdemocracia", na busca do equilíbrio "entre o estado de *laissez faire* permissivo e uma censura disfarçada em nome de uma legislação regulatória", na finalidade de inibir "crimes e desmandos" (Cf.: AGUIAR, Poliana P. de M.; BRENNAND, Edna G. de G. Gestão jurídico-estratégica do cibercrime no contexto da ciberdemocracia. In: BRANT, Cássio (Coord.). **Direito digital & sociedade 4.0**. Belo Horizonte: D'Plácido, 2021, p. 753-780; p. 778.

[363] Numa dimensão simplista (sem esquecer-se dos jogos de linguagem de Ludwig Wittgenstein, em *Investigações Filosóficas*), há "6909 línguas diferentes faladas ao redor do mundo" (Cf.: MOTOMURA, Marina. Quantos idiomas existem no mundo? **Superinteressante**, 25 maio 2011. Disponível em: https://super.abril.com.br/mundo-estranho/quantos-idiomas-existem-no-mundo. Acesso em: 6 jul. 2022).

[364] A dificuldade no âmbito da União Europeia, como na questão da produção da prova penal digital pelas crescentes novas tecnologias, é evidenciada na proposta de um processo penal transnacional. Cf.: SCHÜNEMANN, Bernd. **Estudos de direito penal, direito processual penal e filosofia do direito**. São Paulo: Marcial Pons, 2013, p. 265-281.

[365] BUSATO, **Direito Penal**... *Op. cit*, p. 364.

4.4 OS PROJETOS DE LEI DO BRASIL REFERENTES ÀS INVESTIGAÇÕES CRIMINAIS DIGITAIS CRIPTOGRAFADAS À LUZ DA EXPERIÊNCIA ESTRANGEIRA

Como último ponto de reflexão nesta pesquisa, frente a uma visão dirigida ao constitucional sistema acusatório cada vez mais enraizado no CPP e leis extravagantes, imperativa a revisão da Lei n. 9296/96 e das questões polêmicas até aqui debatidas, mas ainda não normatizadas no Brasil. Em destaque, a responsabilidade penal da pessoa jurídica (provedores) como garantidora da interceptação telemática de mensagens digitais dotadas de E2EE, e, os meios alternativos de investigação da prova penal digital, incluindo a possível manutenção, ou não, da criptografia ponta a ponta. Contudo, há outras inúmeras inserções propostas, como se verá dos inúmeros projetos de lei em trâmite neste país, a seguir considerados, denotando-se a dificuldade de unir todos os elementos necessários para o debate necessário à produção legislativa.

Veja-se, por exemplo, que não há legislação que determine de maneira específica como deve ser a execução prática das interceptações telemáticas, apesar de seus requisitos constitucionais e legais (art. 2º da Lei n. 9296/96) serem os mesmos. Assim, pelo vácuo normativo, por mera questão de método, "convencionou-se determinar aos provedores de e-mails (ou de outras aplicações de trocas de mensagens on-line) a criação de contas espelho,[366]" replicando-se, em tempo real, os fluxos de mensagens dos investigados para o devido acesso pelas autoridades legais, sem prejuízo de outros meios tecnologicamente viáveis. Mas isso não está disciplinado por lei específica, a casos em geral[367], e pode ser questionada judicialmente eventual produção de prova ilícita. Veja-se, a contrário sensu:

> 4. O fato da Polícia Federal ter criado um software para quebrar a chave de criptografia do sistema BBM Messenger não é causa de nulidade processual, pois o art. 53 da Lei 11.343/06 permite a utilização de qualquer meio investigativo previsto em lei — quebra do sigilo telemático, por exemplo, e as normas vigentes não restringem ao fabricante essa atividade, sobretudo diante de crimes graves, até porque as autoridades constituídas não podem ficar à mercê da boa vontade dessas empresas em atender à ordem judicial.

---

[366] QUITO, Carina. As quebras de sigilo telemático no processo penal e o paradoxo do acesso irrestrito às comunicações armazenadas. In: WOLKART, Erik Navarro et al. (Coord.). **Direito, processo e tecnologia**. 2. ed. São Paulo: Thomson Reuters Brasil, 2021, p. 169-170.

[367] TRF-1ª Região, 3ª Turma, Apelação Criminal n. 00362112120154013500. Relator: Juiz Federal Marcelo V. N. Albernaz, julgado em 19 jun. 2018. **E-DJF**, 29 jun. 2018.

A comparação aos preceitos legais e jurisprudenciais do direito estrangeiro tratado no capítulo 3, o qual preza pela mínima discriminação legal do método utilizado pela polícia, ao menos, de forma generalista em face da constante alteração da tecnologia, evidenciam ser este o melhor caminho.

A visão sistêmica do nosso ordenamento jurídico, outrossim, deve ser alvo das interpretações nas propostas do legislador. O art. 3º, *caput*, da Lei n. 9296/96, *verbi gratia*, deveria ser revisitado para se afastar do vigente preceito normativo a possibilidade da atuação de ofício do juiz no papel investigativo próprio da autoridade policial e do Ministério Público[368]. Ademais, pelo caráter normativo cada vez mais universal, para além das fronteiras de cada país, especialmente concretizada em matéria penal e processual penal pela Convenção de Budapeste, deve-se buscar no direito comparado normativas e julgados que se atenham a valores aplicáveis em nosso ordenamento jurídico e que enriqueçam, aperfeiçoem o emprego da lei.

Valioso artigo científico[369], com base nos julgamentos de Cortes internacionais (CADH, CEDH, CIDH e a TEDH), e, nos arts. 268 e seguintes do *Codice di Procedura Penale* italiano[370], realiza propostas de *lege ferenda* da interceptação telefônica e telemática para aperfeiçoar a produção da prova em matéria penal, tal como disposto na Lei n. 9296/96, que vão ao encontro das recentes reformas de nosso CPP quanto à cadeia de custódia da prova (arts. 158-A e seguintes). Nessa toada, traz-se ainda o caso *Tristán Donoso vs. Panamá,* no qual a CIDH demonstrou que o "direito convencional à vida privada, por não ter natureza *absoluta*, pode ser limitado pelos Estados sempre que tal restrição não tenha cariz *abusivo* ou *arbitrário*", devendo estar previsto em lei, um fim legítimo idôneo, necessário e proporcional; e, por fim, elege a interceptação telefônica[371] como uma das medidas judiciais "necessárias no

---

[368] O MPF alegou, em agravo regimental, violação ao sistema acusatório pelo Min. Alexandre de Moraes, pois este determinou, de ofício, medidas cautelares para apurar suposta participação de empresários em atos antidemocráticos. BRASIL. Ministério Público Federal. **MPF aponta vícios e pede anulação de decisão que determinou cautelares contra empresários por conversas em grupo de WhatsApp.** Disponível em: bit.ly/3F4piqd. Acesso em 15 nov. 2022.

[369] Conforme: MALAN, Diogo. Interceptação de comunicações telefônicas: Standards dos sistemas interamericano e europeu de direitos humanos. In: SANTORO, Antonio E. R.; MADURO, Flávio Mirza (Org.). **Interceptação telefônica**: 20 anos da Lei 9.296/96. Belo Horizonte: D'Plácido, 2017. p. 149-174.

[370] ITALIA. **Codice di Procedura Penale**. Disponível em: https://www.polpenuil.it/attachments/048_codice_di_procedura_penale.pdf. Acesso em: 04 dez. 2022.

[371] Regras que se estendem à interceptação telemática, cf. ADPF 403, p. 26.

âmbito de sociedade democrática". Semelhantes são os critérios de exame jurídico em julgados do TEDH sobre interceptações telefônicas.[372]

Não há como discordar, então, que a

> necessidade de legiferação para tutelar o direito à privacidade e à proteção de dados é uma ênfase mundial, e será comum que cada vez mais sejam direcionadas às *bigtechs* em face do tratamento de dados pessoais de forma inadequada ou abusiva, por exemplo[373].

E as propostas legislativas adiante levantadas vão além da mera análise da Lei n. 9296/96, evidenciando-se o intrincado arcabouço jurídico da prova penal digital. Elas passam por reformas dos preceitos do Marco Civil da Internet e da criação da Lei Geral de Proteção de Dados Pessoais em matéria penal (LGPDP), dentre outros inúmeros preceitos jurídicos que passam pelo sistemático estudo dos atos de investigação criminal e a nova era na comunicação de dados.

Em razão da propagação global das novas tecnologias de comunicação digital e da sua repercussão nos direitos fundamentais ligados à intimidade e à vida privada, decidiu o STF (2020), haver um princípio constitucional implícito à autodeterminação informacional[374]. Pouco tempo depois disciplinou o Congresso Nacional, como direito constitucional, a proteção de dados pessoais (inclusive digitais), conforme o art. 5º, LXXIX, da CF (Emenda Constitucional n. 115[375], de 10 de fevereiro de 2022).

Pelos mesmos motivos, foi igualmente reconhecido pelo Tribunal Constitucional Federal da Alemanha esse "reflexo de fenômeno de dimensão global, influenciando de forma generalizada a transformação jurídica concreta dos estados nacionais[376]". E, como análise comparativa, observa-se o quão atrasados estamos nesta toada normativa, tendo em vista que o Tribunal Constitucional Federal da

---

[372] *Op. cit*, p. 154-166.

[373] LÓSSIO, Claudio Joel Brito. **Manual descomplicado de direito digital**: guia para profissionais do Direito e da Tecnologia. 2. ed. São Paulo: JusPodivm, 2021, p. 80.

[374] Conforme STF, na ADI 6387 (Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165. Acesso em: 24 nov. 2022); além de positivado no artigo 2º da Lei n. 13.709/18 (Lei Geral de Proteção de Dados Pessoais - LGPD).

[375] BRASIL. Emenda Constitucional n. 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. **Diário Oficial da União**, Brasília, DF, 11 fev. 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm. Acesso em: 26 out. 2022.

[376] CAMPOS, Ricardo; MARANHÃO, Juliano S. A. Os registros públicos e os fundamentos da proteção de dados (pp. 753-769), p. 762. In: WOLKART, Erik Navarro et al. (Coord.). **Direito, processo e tecnologia**. 2. ed. São Paulo: Thomson Reuters, 2021.

Alemanha já desde 1983[377] (ao declarar inconstitucional a lei do censo estatístico, a qual previa a coleta de dados pessoais) erigiu o "direito à autodeterminação informativa" como inerente à proteção da personalidade, refletindo, pela evolução tecnológica nos anos seguintes, na proteção de dados digitais como um direito fundamental constitucional. Vale frisar que, mesmo diante disso, não se obstou que na Alemanha houvesse profunda reforma do seu direito processual penal para a interceptação telemática de comunicações digitais criptografadas, como visto no subcapítulo 3.3, em destaque a reforma do CPP alemão em 2017.

Outro aspecto que se verifica fazer parte do estudo para o aperfeiçoamento técnico-legislativo nos projetos de lei do Brasil, com o resguardo do Estado Democrático de Direito, é a criação de instrumentos para, apesar de um lado acelerar as investigações de metadados (ausente a reserva jurisdicional), por outro, trazer o controle externo da atividade policial, abrangendo não só os atos de investigação em si (e das interceptações telemáticas autorizadas judicialmente), mas as próprias perícias, inclusive, com a possibilidade de atos de investigação particular[378]. Em consonância a tal recomendação, inúmeros países criaram instrumentos legítimos para tal finalidade, denotando-se uma preocupação transnacional no controle externo da atividade policial investigativa voltado à proteção de dados informáticos; em especial, há diretrizes da ONU e normas de diferentes modelos de controle, tanto do *common law* (Estados Unidos e Reino Unido), como dos sistemas europeus continentais (Alemanha, Espanha etc.)[379].

Toda esta preocupação normativa, tal como nos países já retratados nesta dissertação, também repercute no Brasil e, apesar de estudos escassos sobre os projetos de lei em trâmite sobre toda esta problemática, denota-se que o Poder Legislativo brasileiro está atuante nessas celeumas; logo, imprescindível a apreciação acurada de tais legislações propostas com vistas a sua organização, com base na jurisprudência e normas brasileiras e do direito comparado.

---

[377] Em especial, atualmente, "a garantia jurídico-fundamental da confidencialidade e da integridade dos sistemas técnicos de informação de uso próprio" (Cf.: HOFFMANN-RIEM, Wolfgang. A Proteção Jurídica Fundamental da Confidencialidade e da Integridade dos Sistemas Técnicos de Informação de Uso Próprio. Tradução: Italo R. Fuhrmann. **Direito Público**, Brasília, v. 18, n. 100, out./dez. 2021. DOI: https://doi.org/10.11117/rdp.v18i100.6212. Acesso em: 21 dez. 2022.

[378] Sobre o tema: MACHADO, Leonardo Marcondes. I**ntrodução crítica à investigação preliminar**. Belo Horizonte: D'Plácido, 2020.

[379] A respeito do tema, vide: ÁVILA, Thiago André Pierobom de. **Fundamentos do controle externo da atividade policial**. Belo Horizonte: D'Plácido, 2016, p. 540-562.

Deste modo, imperativa é a exposição dos projetos de lei em tramitação no Brasil, os quais de forma direta ou indireta tratam das investigações criminais por interceptações telemáticas dotadas da tecnologia da E2EE, mediante uma leitura sistemática no ordenamento jurídico nacional e internacional, visão agora enaltecida pela nossa recente adesão à Convenção de Budapeste e mantida a crescente comunicação de dados digitais.

4.4.1 Projeto de lei n. 5285/2009380 e seus apensamentos: "Escutas Telefônicas Clandestinas" e a Responsabilidade dos Provedores

É preciso introduzir que este subcapítulo teve como norte inicial o estudo dirigido somente ao Projeto de lei n. 5285/2009. Contudo, logo se percebeu que são um total de 55 projetos de lei em tramitação conjunta[381] relacionados ao tema central: a Lei n. 9296/96.

Por isso, visando à organização, a presente pesquisa visará somente os projetos de lei pertinentes ao ponto nodal da dissertação e seus contornos, como o tratamento da questão da criptografia e a responsabilidade das empresas provedoras do serviço de comunicação, a fim de se verificar se o mote nacional se dirige à experiência do direito comparado.

Portanto, passa-se a tratar por este projeto legislativo mais amplo (5285/2009), com incursos aos demais quando pertinente.

Pretende o Projeto de lei n. 5285/2009 regulamentar o inciso XII, parte final, do art. 5º da Constituição Federal, ou seja, o que trata da inviolabilidade das comunicações telefônicas, ressalvada sua possibilidade se mediante ordem judicial e nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal (hoje, a sob n. 9296/96, com sua revogação prevista neste projeto de lei em seu art. 31).

Há hipóteses tratando da criptografia em três pontos do projeto de lei: **a)** a responsabilidade criminal, criando-se novo tipo penal em nosso ordenamento jurídico,

---

[380] BRASIL. Câmara dos Deputados. Projeto de Lei n. 5285/2009. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=659491&filename=PL+5285/2009. Acesso em: 26 out. 2022.

[381] *Id.* **Árvore de Apensados - PL 5285/2009**. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_arvore_tramitacoes?idProposicao=436096. Acesso em: 26 out. 2022.

daquele que sem autorização ou em desacordo com determinação legal ou regulamentar, produzir, fabricar, importar, comercializar, oferecer, emprestar, adquirir, possuir, manter sob sua guarda ou ter em depósito, equipamentos destinados especificamente à interceptação, escuta, gravação e decodificação das comunicações telefônicas, incluindo programas de informática e aparelhos de varredura; e, também, se imputa o crime a quem utiliza a criptografia para proteger comunicação de voz, imagem e dados, em desacordo com as normas expedidas pelo órgão federal competente (art. 21, *caput* e parágrafo único); **b)** a fiscalização sob responsabilidade da ANATEL (Agência Nacional de Telecomunicações) do uso da criptografia e de sistemas de interceptação (art. 28, § 1º); **c)** ao eleger também a ANATEL como a depositária da chave de acesso de qualquer comunicação criptografada (art. 28, § 2º).

Evidentemente, essa responsabilização criminal almeja evitar a criação da indústria da "escuta ilegal", cominando pena de reclusão de dois a oito anos e multa.

O projeto não prevê a responsabilidade penal da pessoa jurídica, algo que seria, em tese, juridicamente possível, como exposto no subcapítulo 2.4, cabendo a observação de que não há como fazer uma analogia por seu cabimento da forma como a redação legislativa propõe, tendo em vista a óbvia taxatividade em matéria penal, mas até mesmo pela pena em abstrato cominada, incompatível com as sanções possíveis às empresas responsáveis por "produzir" ou "fabricar", por exemplo, o equipamento de *hacking* nas comunicações digitais ou de escuta ilegal. Quisesse ser diferente deveria o legislador dispor em termos semelhantes ao da Lei n. 9605/98 (arts. 3º, 21 a 23)[382], ou seja, de forma taxativa a responsabilidade penal da pessoa jurídica nos crimes ambientais e as penas compatíveis (restritivas de direitos, prestação de serviços à comunidade e multa).

É omisso o projeto sobre outros métodos de investigação possíveis, tal como o *hacking* estatal; tampouco menciona a tutela da interceptação telemática de forma clara em seu art. 1º ("A interceptação de comunicações telefônicas, de qualquer natureza"), mas de forma esparsa a prevê, parecendo se utilizar do termo "telefônica" como gênero.

---

[382] BRASIL. Lei n. 9605, de 12 de fevereiro de 1998. Dispõe sobre as sanções penais e administrativas derivadas de condutas e atividades lesivas ao meio ambiente, e dá outras providências. **Diário Oficial da União**, Brasília, DF, 13 fev. 1998. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9605.htm. Acesso em: 27 out. 2022.

É preciso lembrar que existem empresas especializadas[383], as quais, a pedido de alguns países, já se noticiou criarem a possibilidade de interceptação telemática mesmo em serviços de mensageria digital dotada de criptografia de ponta a ponta[384]. Muito diferente, e é o intuito que o projeto de lei traz, é a pessoa não autorizada (pela ordem constitucional, legal ou regulamentar) procurar tais empresas especializadas para fornecerem, nos verbos do tipo penal, tais programas visando à escuta ilegal.

No Projeto de lei n. 2934/11, de tramitação em apenso à presente (altera a Lei n. 9.296/96, para dispor sobre a proibição de comercialização de equipamento de interceptação telefônica), tampouco prevê a responsabilidade criminal da pessoa jurídica pela comercialização desses equipamentos, mas uma sanção administrativa com previsão de multa, da seguinte forma[385]:

> Art. 10-C. O fabricante instalado no país, ou o importador, representante ou revendedor do fabricante estrangeiro, fica obrigado a informar à polícia federal, em trinta dias da publicação desta lei, a quem foi vendido equipamento de interceptação telefônica, discriminando, de forma inequívoca, a quantidade e características dos equipamentos e os dados identificadores dos respectivos compradores.
> Parágrafo único. A inobservância do disposto no caput sujeita o infrator à multa de até metade do valor de cada transação omitida, a ser aplicada pelo conselho gestor do Fundo Nacional de Segurança Pública, mediante informação da polícia federal.

Ressalte-se, voltando ao Projeto de lei n. 5285/2009, que a ausência de autorização judicial é tida como crime (art. 22) em tipo penal autônomo ao acima descrito (tal como na atual Lei n. 9296/96, art. 10, aqui com pena máxima em abstrato menor que a da nova proposta de lei: reclusão de 2 (dois) a 4 (quatro) anos, e multa"), e cabível a regra do concurso material de crimes caso ocorrido o fato do art. 21 do

---

[383] São os "produtos chamados de 'software de interceptação legal'" e produzidos por empresas privadas com sedes no Reino Unido e Alemanha (FinFisher), Itália (Hacking Team) e Israel (NSO Group)." (In: RAMIRO, André (Coord.). **O mosaico legislativo da criptografia no Brasil**: uma análise de projetos de lei. Recife**:** IP.Rec, 2020. p. 46.

[384] Vide subcapítulo 3.3, ao falar do hacking estatal na Alemanha.

[385] BRASIL. Câmara dos Deputados. Projeto de Lei n. 2934/11. Altera a Lei n. 9.296, de 24 de julho de 1996, para dispor sobre a proibição de comercialização de equipamento de interceptação telefônica. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=950990&filename=PL+2934/2011. Acesso em: 27 out. 2022.

projeto de lei (art. 69 do CP), tutelando-se a reserva (constitucional) de jurisdição[386] à interceptação telefônica e telemática. Vale a transcrição[387]:

> Art. 22. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática e, ressalvado o uso ostensivo de sistemas de segurança, a captação de imagem e som ambiental por todos os meios, sem expressa autorização judicial. Pena: reclusão, de dois a seis anos, e multa. Parágrafo único. A pena é de reclusão, de dois a oito anos, e multa, se o crime é praticado por policial, servidor ou membro do Ministério Público.

Como exposto, o Projeto de lei n. 5285/2009 prevê modificações da atual Lei n. 9296/96 e sua revogação expressa (art. 31). Os novos requisitos para a interceptação telefônica são muito semelhantes ao já vigentes, acrescidas modificações que estão de acordo com a tendência mundial do resguardo da privacidade, e, sobretudo, sem prejuízo da amplitude de cabimento material da interceptação telefônica e telemática com vistas à produção da prova penal.

Do seu art. 4º, tem-se a previsão da indicação dos métodos a serem empregados e a identificação dos servidores incumbidos à execução da interceptação de comunicação telefônica ou de captação de imagem e som ambiental, a qual deve abranger a técnica de investigação no caso de comunicações digitais (telemática).

Outro ponto que merece ênfase é o art. 11 do projeto, tomando-se em conta a jurisprudência da Suprema Corte norte-americana no caso *Jones v. United States*, de que o acesso ao *smartphone* é equivalente à vida privada quase completa da pessoa investigada, com a manutenção do que já prevê a Lei n. 9296/96 (art. 9º): a exclusão de dados alheios ao interesse da justiça. Merece aqui a crítica de que deveria ser mais claramente prevista a interceptação telemática e o acesso a dados digitais do investigado como abrangido no objeto de tal medida, dada a generalidade de sigilo do art. 1º do projeto (interceptação telefônica), acima já tratada, vindo ao encontro das reivindicações dos defensores da garantia da privacidade.

---

[386] "A reserva de jurisdição impõe-se a situações em que a função do Poder Judiciário não pode ser exercida por qualquer outro poder, porquanto existe a necessidade de se solucionar, de forma definitiva, conflitos de interesses que resultam em restrições a bens constitucionalmente protegidos" (p. 10, cf.: VILARES, Fernanda. **A Reserva de Jurisdição no processo penal**: dos reflexos no inquérito parlamentar. Disponível em: bit.ly/3VB3729. Acesso em: 26 out. 2022).

[387] Projeto de lei n. 5285/2009.

Outrossim, tal como critica a doutrina[388] na reforma no CPP da Alemanha quanto ao *hacking* estatal, o resguardo do direito de sigilo profissional[389] dos fatos objeto de apuração no inquérito policial, ou no processo-crime, deve ser tutelado, prevendo que a gravação captada não poderá ser usada como meio de prova e deve ser inutilizada (art. 13).

Já no art. 14 do projeto há mais uma limitação às investigações criminais (não vedada na Lei n. 9296/96). É o caso da serendipidade (ou encontro fortuito das provas), pois prevê o dispositivo proposto que as interceptações de comunicações telefônicas e captações de imagem e som ambiental, que detectarem, de maneira fortuita, informação de outros crimes e, também, praticados por terceiros que não eram alvo de investigação, não serão aceitas como prova lícita. Já a jurisprudência atual do STJ[390] e do STF[391] são pela legalidade da prova fortuita obtida, desde que obedecidos os ditames constitucionais e legais anteriores (justa causa, ou, fundadas razões), dependente, portanto, do exame de eventual ilegalidade do caso concreto[392], tal como a pescaria probatória (*fishing expedition*) após o ingresso indevido de policiais em residência, gerando a ilicitude das provas assim obtidas. Mas vale mencionar que, no caso de interceptação telemática num *smartphone*, por sua robusta invasão na privacidade do investigado comparada à meramente telefônica, pode passar a ser refutada se houver um exagero na invasão da intimidade, aplicando-se a Teoria do Mosaico, tal como nos precedentes norte-americanos.

A proposta legislativa traz apenas duas exceções à vedação da serendipidade: a) se o indiciado estiver na iminência do cometimento de um delito (*caput*); b) casos de imagens e sons captados por sistemas ostensivos de segurança

---

[388] Vide rodapé n. 245.

[389] Lembrando que, tal como o STF, o STJ pacificou que "a garantia do sigilo das comunicações entre advogado e cliente não confere imunidade para a prática de crimes no exercício da advocacia, sendo lícita a colheita de provas em interceptação telefônica devidamente autorizada e motivada pela autoridade judicial. (STJ, 6ª Turma, REsp 1465966/PE. Relator: Min. Sebastião Reis Júnior. **DJe**, 19 out. 2017).

[390] E, "consideram-se válidas as provas encontradas casualmente pelos agentes da persecução penal, relativas à infração penal até então desconhecida, por ocasião do cumprimento de medidas de investigação de outro delito regularmente autorizadas, ainda que inexista conexão ou continência com o crime supervenientemente encontrado, desde que não haja desvio de finalidade." (STJ, AgRg no AREsp 2037992/SC. Relator: Min. Reynaldo S. da Fonseca, 5ª Turma. **DJe** de 13 set. 2022).

[391] Vide: "Nas interceptações telefônicas validamente determinadas é passível a ocorrência da *serendipidade*, pela qual, de forma fortuita, são descobertos delitos que não eram objetos da investigação originária. Precedentes: HC 106.152, Primeira Turma. Relator: Min. Rosa Weber, **DJe** de 24/05/2016; e HC 128.102, Primeira Turma. Relator: Min. Marco Aurélio. **DJe** de 23/06/2016." (STF, HC 137438, 1ª Turma, Relator Min. Luiz Fux, publicado em 20/06/2017).

[392] Conforme: STJ, HC 732986/SC, Relator Desembargador Convocado Olindo Menezes, 6ª Turma, **DJe** de 17/10/2022, 17 out. 2022.

(parágrafo único). Nesta exceção, é a como aceita nos julgados dos EUA sobre a leitura de placas de veículos em rodovias (ALPRS) e câmeras de vigilância policial na residência de suspeitos por câmera de captação infravermelha, porém, sob os limites da 4ª emenda, os quais podem ser aplicados no Brasil.

Por fim, como já aduzido, da apreciação da tramitação legislativa do Projeto de lei n. 5285/2009, verificam-se outros diversos correspondentes e com modificações na Lei n. 9296/96. Desse modo, merecem incurso os projetos legislativos logo após relacionados, ligados aos temas da interceptação telemática e da criptografia.

4.4.1.1 Projeto de lei n. 1394/2021393: em defesa da previsão exemplificativa de métodos tecnológicos

Neste projeto importa aludir a pretensão de acrescentar o art. 9º-A à Lei n. 9.296/96 em ponto coincidente conclusivo desta dissertação, após a análise da doutrina e legislação de outros países. Refere-se à previsão por lei dos métodos de tecnologia empregados para o sucesso da interceptação telemática de maneira genérica, não exaustiva ou exemplificativa, justamente em razão da adaptação em velocidade incompatível com eventual novo trâmite de criação de lei, ressalvada a obediência da cadeia de custódia, a qual também deve estar por regras claras e pré-estabelecidas, de forma que não gere a possibilidade da ilicitude da prova.

Assim sendo, andou bem o legislador ao propor (art. 9º-A desse projeto) que a

> interceptação de comunicações em sistemas de informática e telemática **poderá ocorrer por qualquer meio tecnológico disponível desde que assegurada a integridade da diligência** e poderá incluir a apreensão do conteúdo de mensagens e arquivos eletrônicos já armazenado em caixas postais eletrônicas ou em serviços de armazenamento em nuvem ou similares.

E isso é corroborado da leitura da justificativa do legislador ao projeto, no sentido de que o objetivo do art. 9º-A é, justamente, aperfeiçoar a intenção do Ministério da Justiça e Segurança Pública para incluir outras soluções tecnológicas,

---

[393] BRASIL. Câmara dos Deputados. Projeto de Lei n. 1394/2021. Altera a redação do artigo 5º e acrescenta o art. 9º-A à Lei 9.296 de 24 de julho de 1996 (Lei de Interceptações Telefônicas). Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2278011. Acesso em: 27 out. 2022.

de forma ampla, propiciando a melhor possível à época das investigações, dada a obsolescência programática usual em sistemas informáticos, com a ressalva da preservação da cadeia de custódia.

4.4.1.2 Projeto de lei n. 2942/2015[394]: o contraditório diferido ao investigado

Este projeto acrescenta o § 4º ao art. 6º da Lei 9296/96 para tornar obrigatória, após cumprida a diligência de interceptação telefônica, a notificação do investigado sobre os elementos colhidos, os motivos que justificaram a interceptação e o prazo de sua duração.

Na legislação HB 57/2019 (Utah, EUA)[395] também se prevê tal notificação ao investigado, indo ao encontro da transparência do processo investigativo e o contraditório diferido, inclusive para eventual responsabilização por abusos, excessos policiais e outras ilegalidades ou mesmo teses técnicas defensivas quanto à prova obtida.

4.4.1.3 Projeto de lei n. 3372/2021[396]: o "espelhamento" como meio de obtenção da prova digital

Pretende o projeto modificar a Lei n. 9.296/96 para acrescentar a possibilidade da interceptação das comunicações em sistemas de envio de mensagens instantâneas e chamadas de voz, notadamente, casos do WhatsApp e o Telegram (art. 1º).

Semelhantemente ao projeto de lei tratado no subcapítulo 4.4.1.2, porém, de forma mais detalhista, descreve o meio tecnológico de execução da medida: o "espelhamento". Vale colacionar a proposta:

---

[394] *Id.* Projeto de Lei n. 2.942/2015. Prorroga o prazo para a disposição final ambientalmente adequada dos rejeitos de que trata o art. 54 da Lei n. 12.305, de 2 de agosto de 2010. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1383505&filename=PL+2942/2015. Acesso em: 27 out. 2022.

[395] Conforme subcapítulo de n. 3.1.5.1.2.

[396] *Id.* Projeto de Lei 3.372/2021. Altera a Lei n. 9.296, de 24 de julho de 1996, que regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal, para dispor sobre a interceptação das comunicações em sistemas de envio de mensagens instantâneas e chamadas de voz. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2082264&filename=PL+3372/2021. Acesso em: 27 out. 2022.

> Art. 1º-A. A interceptação do fluxo de comunicações em sistemas de envio de mensagens instantâneas e chamadas de voz poderá ocorrer por meio de:
> I — habilitação, pela operadora de telefonia, em horários determinados, de módulo de identificação de assinante (cartão "SIM") fornecido pela autoridade policial, em substituição àquele utilizado pelo investigado ou acusado;
> II — **espelhamento**, pela autoridade policial, em dispositivo próprio, das mensagens recebidas e enviadas pelo investigado ou acusado.
> Parágrafo único. **A interceptação prevista neste artigo dar-se-á por meio de sistema que assegure a não interferência da autoridade policial nas comunicações travadas pelo investigado ou acusado, seja por meio da exclusão, da edição ou do envio de mensagens**. (Grifo nosso).

Como descrito no parágrafo único (art. 1º-A), segue-se algo parecido ao que se dá no uso do WhatsApp Web, utilizado na Alemanha e rechaçado pelo STJ[397]. A ressalva do STJ é justamente a advertência de que o uso do espelhamento pelo WhatsApp Web é inservível à prova penal em face da possibilidade de inserções nas comunicações digitais por terceiros, e, a proposta legislativa, traz esta condição de não interferência policial. Impossível tal solução, a prova pode ser considerada ilícita, segundo o STJ.

É preciso lembrar, todavia, como já arguido no subcapítulo 3.3, que tal posicionamento pode ser alterado por ressalva ao caso em concreto, pela dependência de todo um conjunto probatório (perícia no aparelho investigado e outros participantes da comunicação digital, por ex.) e o próprio STJ entender que a violação da cadeia de custódia não implica, de maneira obrigatória, ou, automaticamente, a inadmissibilidade ou a nulidade da prova colhida.

4.4.2 Projetos de lei relativos ao Marco Civil da Internet e à E2EE

Esgotada a análise acima quanto aos projetos de lei atinentes à Lei n. 9296/96, passa-se aos concernentes à criptografia de forma mais incisiva, especialmente, com modificações na Lei n. 12.965/14, o conhecido Marco Civil da Internet.

---

[397] Conforme rodapé n. 269.

4.4.2.1 Projeto de lei n. 9808/18398: as celeumas da E2EE, o STF e o direito comparado

Este projeto legislativo acrescenta ao art. 10[399] da Lei n. 12.965/14, os parágrafos 5° e 6º, a fim de dispor sobre o acesso ao conteúdo dos dados de comunicação privada por meio de aplicativos de internet para fins de persecução criminal. Trata, expressamente, da criptografia.

Pertinente a transcrição da proposta:

> § 5º — Encontrando-se o agente em situação **flagrante** de crimes definidos em lei como **hediondo, de tráfico de drogas ou terrorismo**, poderá **o delegado de polícia acessar, independente de autorização judicial, os dados de registro e conteúdos de comunicação privada de dispositivo móvel,** quando necessário à investigação e/ou à interrupção da ação delitiva.
> § 6º — No caso do parágrafo anterior, **em se tratando de dados criptografados, poderá o delegado de polícia requisitar, diretamente aos provedores de internet, provedores de conteúdo e autores de aplicativos de comunicação, o fornecimento de chave criptográfica** que permita o acesso aos dados e **conteúdos de comunicação privada de dispositivo móvel**, **sem prejuízo do desenvolvimento** e emprego, pelas polícias judiciárias, **de técnicas e ferramentas tecnológicas que atinjam esse fim específico**, incluindo a utilização de dispositivos que possibilitem o acesso a conteúdo anterior à **criptografia** por meio de aplicativos, sistemas ou outras ferramentas. (Grifo nosso).

A redação é clara quanto à pretendida quebra da criptografia por fornecimento de chaves pelos provedores. Neste aspecto, o projeto pode perder parte de seu objeto por eventual decisão contrária do STF na ADPF 403 e na ADI 5527; ou, alterar sua redação por emendas do legislador para outras formas tecnológicas de realizar a interceptação telemática das comunicações digitais dotadas da E2EE.

Pretende-se no projeto, sob a justificativa de crime em estado de flagrância, o afastamento do princípio da reserva da jurisdição para a interceptação telemática, o

---

[398] *Id.* Projeto de Lei n. 9.808/2018. Acrescenta os parágrafos 5° e 6º ao art. 10 da Lei n. 12.965, de 23 de abril de 2014, para dispor sobre o acesso a dados de comunicação por meio de aplicativos de internet para fins de persecução criminal, nos casos que especifica. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1649924. Acesso em: 28 out. 2022.

[399] "Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e **do conteúdo de comunicações privadas**, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas" (MCI).

que deve ser afastado pela sua inconstitucionalidade, além do entendimento jurisprudencial das Cortes brasileiras em sentido contrário[400].

Deve ser lembrado que, nem mesmo na já citada lei de Utah (H.B. 57/2019)[401], e as ressalvas da jurisprudência norte-americana das chamadas "circunstâncias exigentes"[402] para acesso a dados do celular do preso, permite-se à autoridade policial (sem mandado judicial) o acesso ao conteúdo de conversas, dotadas ou não da E2EE, mas somente a informações de localização do dispositivo eletrônico.

A Suprema Corte dos EUA afastou a tese de ser uma exceção à garantia da 4ª emenda a análise do celular do preso no caso Riley v. Califórnia em hipóteses que ali se discrimina, como exposto no subcapítulo 3.1.3, especialmente, a idêntica ao projeto de lei ora em análise: descabe a tese do governo da busca desprovida de mandado judicial no celular de um preso quando, simplesmente, entender o policial ser razoável acreditar que o telefone tivesse evidências do crime da prisão ocorrida, motivando no referido julgado que essa ação não é adequada nesse contexto (*smartphones*) e não se revelaria nenhum limite prático quando se trata de buscas de telefones celulares (sentidos quantitativo e qualitativo das informações do cidadão); como resultado, acabaria legitimando sempre a busca no *smartphone* sem mandado judicial.

O acesso indiscriminado ao celular do preso em flagrante, ainda que em crimes graves, pode gerar a ilicitude das provas e de todas as dela decorrentes, a depender do caso concreto. Aliás, o rol de crimes do projeto abrange qualquer crime de tráfico, sabendo-se que a maioria de sua ocorrência na prática forense são de pequena monta, como o privilegiado (art. 33, § 4º, da Lei 11.343/06[403]); os crimes hediondos são vários e seria levado em conta, assim, sua periculosidade em abstrato, não no caso concreto, como nos precedentes relativos à legítima defesa da vítima ou terceiros, assim como no caso de terrorismo em caso extremo de perigo iminente decorrente de uma bomba em local público lotado de pessoas. Em suma, deve-se, no mínimo, haver uma circunstância, de fato, exigente, de um ato do delegado compatível

---

[400] Tal como os julgados dos rodapés n. 280 e n. 282.

[401] Vide subcapítulo n. 3.1.5.1.2.

[402] Conforme comentário do caso Riley v. Califórnia e rodapé n. 157 ("exceções "de perigo" à 4ª emenda, de segurança nacional ou perecimento de provas imediatas").

[403] BRASIL. Lei n. 11.343, de 23 de agosto de 2006. Institui o Sistema Nacional de Políticas Públicas sobre Drogas - Sisnad; [...]. **Diário Oficial da União,** Brasília, DF, 24 ago. 2006. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11343.htm. Acesso em 28 out. 2022.

à afronta constitucional do sigilo telefônico, sob pena de se vulgarizar uma medida excepcional.

Quanto ao acesso aos metadados[404], o projeto de lei está de acordo com o ordenamento jurídico.

De qualquer forma, apesar dessas críticas, não há impedimento de emendas ao projeto de lei para adaptá-la em tais pontos, assim como em relação ao julgamento pendente do STF nas aludidas ações constitucionais (ADPF 403 e ADI 5527). Revela-se a tendência mundial da taxatividade e o entendimento inicial do Legislativo da ausência de um direito absoluto em face do conflito de direitos e garantias fundamentais da intimidade e privacidade em face da segurança pública, como se verifica da leitura da justificativa do projeto. Ponto positivo é a possibilidade de prever-se, através de lei, alternativas tecnológicas para a interceptação telemática nos casos da E2EE.

4.4.2.2 Projeto de lei n. 6960/2017[405]: um comparativo ao novo alcance da 4ª emenda

Prevê este projeto alterações no Marco Civil da Internet visando elastecer o alcance da tutela privada das pessoas a novas hipóteses tecnológicas, atuais e futuras, que abarcam a esfera da intimidade em prol do disposto no art. 5º, X, da Constituição Federal.

Assim, resguarda-se, tal como no direito norte-americano sob a sua 4ª emenda (na abrangência do termo "*effects*"[406]), não só "o computador ou qualquer dispositivo que se conecte à internet" (na redação atual do MCI, art. 5º, II). Acrescenta o projeto, a esta redação, maior abrangência: "podendo esse dispositivo ser móvel (celulares, *smartphones*, *tablets* ou similares), ou fixos, que não possibilitem o deslocamento do dispositivo conectados à internet de forma concomitante".

---

[404] Conforme o art. 13-A do CPP, lembrando-se que os metadados não são criptografados (vide o rodapé n. 43).

[405] BRASIL. Câmara dos Deputados. Projeto de Lei n. 6960/2017. Alterar a Lei n. 12.965 de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, alterando o art 5°, inciso II e o art 7°, inciso III. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1526689&filename=PL+6960/2017. Acesso em: 28 out. 2022.

[406] Vide rodapé n. 128.

Deixa-se ainda claro que é direito do usuário a inviolabilidade e o sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial, acrescendo-se, no projeto legislativo, os "terminais fixos ou móveis" (art. 7º, III, do MCI).

O objetivo, destarte, dessas alterações, seguindo a justificativa do legislador, é ditar o limite do poder de polícia nas abordagens investigativas criminais, seguindo julgados das Cortes superiores de sua ilicitude no acesso de dados em celulares, sem a devida ordem judicial, como regra.

4.4.2.3 Projeto de lei n. 11.007/2018[407]: a obtenção de prova penal digital sob o pretexto de atos terroristas

Regulamenta este projeto questões sobre o terrorismo, ligadas à investigação criminal e meios de obtenção de prova, medidas de prevenção ao aumento de atores terroristas, alterando a Lei n. 13.260/16 (Lei Antiterrorismo). O projeto não prevê, diretamente, o tema dos dados de mensageria digital com criptografia ponta a ponta, contudo, criminaliza condutas a ela relacionadas.

Da justificativa do projeto por parte do legislador proponente, argumenta-se ser necessária a atualização da Lei n. 13.260/2016, bem como os meios de investigação criminal e obtenção de prova. A novidade proposta é considerar crime o ato de colaborar com informação ou vigilância de pessoas, bens ou instalações, bem como a prestação de serviços tecnológicos, nos seguintes termos:

> Art. 6º — Praticar qualquer ato de colaboração com as atividades ou as finalidades de uma organização, grupo ou elemento terrorista, ou para a prática de qualquer dos delitos previstos nesta lei.
> Pena- reclusão, de cinco a dez anos e inabilitação para o exercício de cargo, emprego ou função por idêntico período.
> § 1º — Consideram-se atos de colaboração **a informação ou vigilância de pessoas**, bens ou instalações, a construção, cessão ou utilização de alojamentos ou depósitos, a ocultação, acolhimento ou traslado de pessoas, a organização de práticas de entretenimento ou assistência a elas, **a prestação de serviços tecnológicos, e qualquer outra forma equivalente de cooperação ou ajuda às atividades das organizações ou grupos terroristas, grupos ou pessoas a que se refere o parágrafo anterior**. (Grifo nosso)

---

[407] BRASIL. Câmara dos Deputados. Projeto de Lei n. 11.007, de 2018. Regulamenta o disposto no inciso XLIII do art. 5º da Constituição Federal, define terrorismo, dispõe sobre investigação criminal e meios de obtenção de prova, [...]. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1696507. Acesso em: 28 out. 2022.

Sugere-se no projeto meios de obtenção de prova condizentes à evolução social e ao armazenamento de provas digitais, visando atos do chamado terrorismo digital (ou ciberterrorismo) nacional e transnacional (alteração do seu art. 8º, §1º), ausentes na lei atual, evidenciando-se aqui a importância da Convenção de Budapeste e, talvez, uma regulamentação genérica, como as previstas no Marco Civil da Internet, não somente para crimes de terrorismo, relembrando-se que não se deve prever hipóteses somente baseadas na gravidade em abstrato do crime. Veja-se do projeto o destaque às provas digitais:

> Art. 8º [...] §1º — Em qualquer fase da investigação e da persecução penal, serão permitidos os seguintes meios de obtenção de prova: [...]
> IV – acesso a **registro** de ligações telefônicas e telemáticas, a **dados cadastrais** constantes de bancos de dados públicos ou privados e a informações eleitorais ou comerciais;
> V — **interceptação de comunicações telefônicas e telemáticas, nos termos da legislação específica**; (Grifo nosso).

Por fim, a celeuma das "circunstâncias exigentes", tal como tratada na jurisprudência e doutrina norte-americana, não aparece em momento algum deste projeto, fator relevante que deve ser objeto de futura legislação, ainda que de forma genérica (não exaustiva), ou como acréscimo no Marco Civil da Internet, para posterior enquadramento ao caso concreto.

4.4.2.4 Projeto de lei n. 2418/2019[408]: os deveres dos provedores na fiscalização de atos de terrorismo e a possibilidade do *hacking* estatal

Na linha do Projeto de lei n. 11.007/18, acima retratado, o presente almeja tutelar o problema do ciberterrorismo, mas agora, voltado à alteração do MCI, criando um dever aos provedores de aplicações de internet: o monitoramento de atividades terroristas e crimes hediondos nos moldes da Lei n. 13.260/16.

Acrescenta ao MCI o seguinte dispositivo:

> Art. 21-A. Os **provedores** de aplicações **deverão monitorar ativamente publicações** de seus usuários que impliquem **atos preparatórios ou ameaças de crimes hediondos ou de terrorismo**, nos termos da Lei nº 13.260/2016.
> [...]

[408] *Id.* Projeto de Lei n. 2418/2019 Altera a Lei n. 12.965/2014, para criar obrigação de monitoramento de atividades terroristas e crimes hediondos a provedores de aplicações de Internet e dá outras providências.Disponível:https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1735011&filename=PL+2418/2019. Acesso em: 28 out. 2022.

> § 3º Na **impossibilidade eventual e justificada de cumprimento do disposto no *caput*, os provedores de aplicações deverão permitir a instalação de softwares ou equipamentos pelas autoridades competentes que permitam o monitoramento para o mesmo fim.**

Observa-se alteração substancial da função do provedor com a introdução do art. 21-A do MCI, pois, sob pena de responsabilidade civil, passa a ter função proativa, de fiscalização, independentemente de qualquer notificação da parte interessada, como prevê o vigente art. 21 da lei[409], o qual também prevê que tal responsabilidade tem a condicionante da possibilidade técnica de agir da pessoa jurídica (em harmonia ao que se verifica no direito comparado quanto à E2EE), objeto este de crítica dos defensores de um método que possibilite a investigação criminal, porque perpetua uma escusa de interesse empresarial de descumprimento de ordens judiciais pela alegada quebra impossível da criptografia.

Mas, nesse projeto, a aludida ressalva, pelo que se indica do proposto art. 21-A do MCI ao se inclinar a um direito à investigação criminal, cai por terra. É que, pelo seu §3º, permite-se, expressamente, a instalação de cavalos de Tróia ou outra tecnologia pelo Estado (*hacking*), capaz de cumprir o dever imposto no seu *caput*. Tal normativa coaduna-se com a nova redação do CPP da Alemanha, conforme subcapítulo 3.3.

E, na forma do art. 3º do projeto, seguindo a sistemática alemã, traz-se a infiltração *online* de agentes dos órgãos de inteligência e dos órgãos de segurança pública, ou seja, nas redes de comunicações telefônicas ou telemáticas, no intuito de realizar o levantamento, processamento e análise de informações acerca de ataques terroristas e homicidas (além de outros delitos), mediante prévia autorização judicial fundamentada.

Há duas hipóteses de fiscalização pelo Estado, portanto, nos arts. 21-A e 3º, ambos deste projeto. Aquele, na primeira parte, volta-se a redes públicas de internet (fóruns *online* e redes sociais), e, o art. 3º, pode abranger a interceptação telemática de *smartphones*, dentre outros, isto é, atos ligados à intimidade das pessoas nas suas conversas telefônicas ou de mensageria privada digital.

---

[409] MCI: "Art. 21. O **provedor** [...] será **responsabilizado subsidiariamente** pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado **quando, após o recebimento de notificação** [...] **deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo**." (Grifo nosso).

Na justificativa do projeto há, cabe frisar, o adendo que já se levantou no início desta dissertação sobre a necessária cooperação das empresas privadas na função censora ligada à segurança pública como um norte provável; aliás, os próprios *sites* de redes sociais e buscadores, além de provedores de aplicações, já reconhecem essa responsabilidade, especialmente, voltada ao terrorismo. E tanto é assim que já foi criado o *Global Internet Forum to Counter Terrorism*[410] (Fórum Global de Combate ao Terrorismo), possuindo parte desses objetivos.

4.4.2.5 Projeto de lei n. 4442/2019[411]: os poderes de investigação digital policial, a Teoria do Mosaico e a responsabilidade penal dos provedores

O Projeto de lei n. 4442/2019 altera o Marco Civil da Internet para estabelecer à autoridade policial a possibilidade de requisição direta de metadados aos provedores.

O vigente art. 10, *caput* e §§ 1º e 2º, disciplina a reserva de jurisdição não só sobre o conteúdo do sigilo de comunicações privadas por parte dos provedores responsáveis (na forma da Lei n. 9296/96), mas também, quanto aos metadados ("dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal").[412] Rememore-se que, em análise do que hoje é vigente no MCI, preconiza a doutrina que o fornecimento de informações pelos provedores de internet é meio probatório (englobados aqui tanto os provedores de conexão ou de acesso à internet, quanto os de aplicações de internet, como as empresas de e-mail, aplicativos de mensagens, armazenamento em nuvens, lojas online etc.), impondo-se o dever legal às empresas de telefonia que fornecem serviços de internet móvel a

---

[410] GLOBAL INTERNET FORUM TO COUNTER TERRORISM (GIFCT). Disponível em: https://gifct.org/. Acesso em: 01 nov. 2022.

[411] BRASIL. Câmara dos Deputados. Projeto de Lei n. 4442/2019. Altera a Lei n. 12.965, de 23 de abril de 2014, para estabelecer a autoridade policial a requisição de dados. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1789130&filename=PL+4442/2019. Acesso em: 01 nov. 2022.

[412] MCI, art. 10, § 1º: "O provedor responsável pela guarda **somente será obrigado** a disponibilizar os registros mencionados no **caput,** de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, **mediante ordem judicial**, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º."

identificação do conteúdo e usuário[413], obedecidos os requisitos legais[414], somente por ordem judicial.

A nova redação proposta ao § 1º do art. 10, esclarece a possibilidade de "requerimento da autoridade policial ou do próprio titular usuário", tanto que, no § 3º, o projeto amplia o rol de pedidos administrativos para "qualquer dado ou informação existente, transação, registro de acesso ou informação de geolocalização, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição", anteriormente, limitado à "qualificação pessoal, filiação e endereço". Tal pretensão é corroborada ainda nos artigos 13, §7º, 15, § 3º e 19, § 1º, todos do projeto ora em comento.

Logo, a partir do projeto de lei, passa-se a englobar os dados obtidos com a "geolocalização" (v.g. pelo histórico de localização do usuário através do Google[415]), como em caso análogo julgado pela Suprema Corte norte-americana: o precedente Jones (c.f. o subcapítulo 3.1.2, quando um dispositivo de GPS foi instalado no veículo do investigado). Aqui, portanto, deve-se levar em conta pela justiça brasileira a Teoria do Mosaico para, a depender do caso concreto (extensão de prazo do monitoramento, ou, apenas uma ou duas datas para apurar onde estava o acusado no momento do crime), seja necessária ordem judicial para a não haver ilicitude na prova produzida, pelo grau de invasão na expectativa de privacidade do investigado por uma série de atos documentados ao serem reunidos.

Outra novidade do projeto proposto é tratar da regra vigente no *caput*, do art. 18, do MCI, o qual dispõe que descabe a responsabilidade civil ao provedor de conexão à internet por danos decorrentes de conteúdo gerado por terceiros, com a ressalva do atual art. 19, mas dentro dos limites técnicos possíveis (aqui, reitere-se, isentaria de responsabilidade as empresas do dever de quebra da criptografia ponta a ponta, pela alegada impossibilidade técnica de acesso a mensagens de usuários, como é o caso do WhatsApp e Telegram):

---

[413] THAMAY, Rennan; TAMER, Maurício. **Provas do Direito Digital**: conceito da prova digital, procedimentos e provas digitais em espécie. São Paulo. Revista dos Tribunais. 2020, p. 138-140.

[414] Arts. 5º; 10; 13, § 5º; 15, § 3º; 22; todos do MCI.

[415] Há projeto de lei do Senado, o qual estabelece que o juiz, a pedido da autoridade policial ou do Ministério Público, poderá determinar que as prestadoras de serviços de telecomunicações forneçam dados que permitam o rastreamento físico de celulares para fins criminais (Projeto de Lei n. 456, de 2015. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/122252. Acesso em: 11 nov. 2022).

> Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser **responsabilizado civilmente** por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e **nos limites técnicos** do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.[416] (Grifo nosso)

Acrescenta-se ao projeto, por fim, a responsabilidade criminal no art. 18, §3º, nos casos de fraude evidente, e, pela falta de cumprimento de um dever dos provedores de conexão da requisição da autoridade policial:

> Art. 18 [...]
> § 1º Com objetivo de combater a hospedagem, acesso e disponibilização de conteúdo fraudulento ou infringente, inclusive fora do Brasil, o delegado de polícia poderá requisitar aos provedores de conexão e independente de ordem judicial, a indisponibilidade ou bloqueio de acesso ao referido serviço, devendo a requisição ser cumprida em 48 (quarenta e oito) horas.
> § 2º A requisição de que trata o caput deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como fraudulento ou infringente, que permita a localização inequívoca do material.
> § 3º O descumprimento à requisição nos casos de fraude evidente, acarretará em responsabilidade civil e **criminal**.

A responsabilidade penal dos provedores de conexão, destarte, seguiria a tendência mundial, apesar de ausente a imputação específica de uma figura delitiva na redação; de qualquer forma, padroniza-se uma intenção de sua criminalização, tal como pretendido nos EUA e Reino Unido.

4.4.2.6 Projeto de lei n. 2419/2022[417] e a valoração da prova ilícita digital (hackeamento do Telegram) em benefício do réu pelo STF

Apensado a outros projetos de lei que tratam do mesmo tema (v.g. o de n. 6518/2019)[418], optou-se por proferir comentários deste, porque mais recente e abrangente em sua redação, projetando alteração na lei vigente, que beneficia

---

[416] BRASIL. Lei n. 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União,** Brasília, DF, 24 abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 11 nov. 2022.

[417] BRASIL. Câmara dos Deputados. Projeto de Lei n. 2419/2022. Possibilita a utilização da captação ambiental feita por um dos interlocutores tanto em matéria de defesa quanto de acusação. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2206050. Acesso em: 11 nov. 2022).

[418] *Id*. Projeto de Lei n. 6518/2019. Altera o § 4º do Art. 8º- A da Lei n. 9.296, de 24 de julho de 1996, para autorizar a captação ambiental como prova lícita tanto por parte da defesa como da acusação. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1848504. Acesso em: 11 nov. 2022).

somente a defesa. O Projeto de lei n. 2419/2022 repercutirá, implicitamente, no tratamento da E2EE, e diretamente, na alteração do art. 8º-A, §4º, da Lei n. 9296/96[419], abarcando não só a Defesa, mas também, a Acusação:

> Art. 8º-A [...] § 4º A **captação ambiental** feita por um dos interlocutores sem o prévio conhecimento da autoridade policial ou do Ministério Público poderá ser utilizada, tanto em matéria de defesa **quanto de acusação**, quando demonstrada a integridade da gravação. (Grifo nosso)

O intuito maior dessa constatação é trazer ao enriquecimento do debate algo ainda que não sobreveio no exame do direito comparado verificado nos capítulos iniciais deste estudo. É que há caso concreto criminal relevantíssimo tratando não da captação ambiental[420], mas da possibilidade de aceitação da prova ilícita em benefício do réu em interceptação telemática ilegal (*hacking online*): o julgamento pela Suprema Corte brasileira da suspeição do então Juiz Federal Sérgio Fernando Moro, tendo em conta na motivação a prova ilícita, produzida por hackers ao invadirem grupo do Telegram utilizados pelo aduzido magistrado e Procuradores da República atuantes da famosa Operação Lava Jato[421].

Ora, a nova redação do art. 8º-A, § 4º, da Lei de Interceptação Telefônica, poderia seguir raciocínio idêntico para a interceptação telemática[422]? O objetivo da resposta é legitimar, ou não, o uso do *hacking* estatal de alguma maneira, retornando às mãos do Estado o gerenciamento da investigação criminal, tal como na Alemanha, independente de cooperação dos particulares, das empresas (em geral *Big Techs*) envolvidas na prova digital almejada. Se possível para a Defesa beneficiar-se da prova ilícita, pois ausente autorização judicial na interceptação de mensagens do grupo do Telegram no precedente acima citado, não seria incongruente, se prevista em lei e

---

[419] Pacificado no STJ que a "gravação ambiental, realizada por um dos interlocutores, é lícita, tendo como condição apenas causa legal de sigilo ou reserva de conversação. (STJ, AgRg nos EDcl no REsp 1843519/MA. Relator: Min. Joel Ilan Paciornik, 5ª Turma. **DJe**, 07 jun. 2021). Tal como o Tema 237 STF: "É lícita a prova consistente em gravação ambiental realizada por um dos interlocutores sem conhecimento do outro".

[420] Sobre a diferença entre interceptação telefônica (art. 5º, XII, da CF)) e gravação "clandestina" (ambiental), esta, admitida como prova lícita gravada por um dos interlocutores sem o conhecimento do outro e ausente causa legal de sigilo ou de reserva da conversação, vide: STF, 2ª Turma, RE 402717-8/PR. Relator: Min. Celso Peluso, julgado em 02 de dezembro de 2008. **DJe**, 13 fev. 2008.

[421] BRASIL. Ministério Público Federal. **Caso Lava Jato.** Disponível em: https://www.mpf.mp.br/grandes-casos/lava-jato/entenda-o-caso. Acesso em: 04 nov. 2022.

[422] Da leitura da justificativa do legislador no Projeto de Lei n. 6.518/19 vê-se a mistura dos termos interceptação telefônica e gravação ambiental, o que é, sabidamente, um equívoco, ao mencionar a Lei n. 9296/96 seguida de precedentes sobre a gravação ambiental e a "interceptação ambiental" (p. 3).

obedecida a reserva de jurisdição para fins lícitos a produção da prova penal digital pelo Estado por igual metodologia? Soa desigual, inicialmente, a resposta negativa, exceto por ressalvas técnicas, mas genéricas e insustentáveis pelas razões expostas no subcapítulo 2.2, e reiteradamente alegadas pelos defensores de manutenção da E2EE nos softwares de mensageria privada. O interesse legítimo da Defesa é o mesmo da Acusação na busca de elementos de seu ônus acusatório (art. 156, *caput*, do CPP), sob um olhar inicial de conflito de direitos e garantias fundamentais.

Autorizado o uso de *hackers* em celulares de magistrados e membros do Ministério Público, ou ainda, de advogados assistentes de acusação, mesmo em nome do direito à ampla defesa do acusado, ausente mandado judicial, abarcando informações ligadas não só ao caso concreto do processo-crime, mas de toda a vida dos interceptados ilegalmente, poderia ser aceito em face dos demais direitos constitucionais envolvidos? A questão é tormentosa, há exceções já há tempos julgadas pela nossa Suprema Corte inclusive (tal como a legítima defesa da vítima), bem lembradas nos votos dos Ministros no julgamento do caso aqui proposto como base de estudo. Daí a explicável votação divergente no STF (placar: 7 a 4), e, o projeto de lei ora em comento para incluir a possibilidade da isonomia à produção da captação ambiental em prol da Acusação.

Uma breve exposição do julgamento no STF e de posicionamentos antagônicos merecem, portanto, ser expostos, pois são dados importantes para entender o raciocínio para se legitimar, ou não, o uso de novas tecnologias pelo Estado para, mantida a E2EE nos aplicativos de mensageria digital, realizar a interceptação telemática nos moldes da Lei n. 9296/96 de forma constitucional, tal como na Alemanha, e, independentemente do resultado da discussão das ações constitucionais sobre o bloqueio do WhatsApp (ADPF 403 e ADI 5527) e de um juízo de ponderação de direitos e garantias fundamentais, o qual, fosse perfeito, não geraria as divergências de entendimentos nos votos, tampouco na própria doutrina.

Na realidade, são dois os feitos julgados na Suprema Corte a respeito de ser ou não possível o uso das conversas no Telegram, obtidas criminalmente por *hackers,* serem admitidas como prova em prol da Defesa por arguição de suspeição do

magistrado: a) HC 164.493[423] (a 2ª Turma reconheceu a suspeição); b) HC 193.726[424] (originário da 2ª Turma, após recursos, levado ao Plenário da Corte, o qual confirmou a decisão pela incompetência da 13ª Vara Federal de Curitiba e a remessa dos processos para a Justiça Federal do DF). A motivação dos votos acerca da utilização da prova ilícita advém de ambos os julgamentos, a seguir resumidos.

O Exmo. Min. Ricardo Lewandowski[425] (vogal no HC 164.493), em seu voto, dividiu sua motivação em capítulo expresso que chamou de "viii) Comunicações espúrias do ex-juiz" (p. 66 e seguintes). Neste, ponderou como argumentos da suspeição, além de outros vários nos ítens anteriores: **a)** que ao menos a existência das mensagens entre os interlocutores não foi por eles desmentidas, além de trazidas aos autos por obtenção de prova pericial da polícia federal relativos à investigação e posterior ação penal contra tais *hackers*, a denominada Operação *Spoofing* (STF, PET 8.290/DF; com denúncia por 176 crimes do art. 154-A, § 3º, do Código Penal[426])[427], perícia a qual atestou ter sido mantida a cadeia de custódia das mensagens extraídas dos celulares das vítimas e mantidos todos os seus dados; **b)** os fatos notórios (mensagens do Telegram trazidas pela mídia) não precisam ser provados, de acordo com o art. 374, I, do CPC; **c)** passa a transcrever vários diálogos escritos entre o então juiz federal e os membros do Ministério Público Federal, prova produzida ilicitamente pelos *hackers*, a fim de trazer elementos de parcialidade judicial para a condenação do réu; **d)** declarou a nulidade de todos os atos processuais, desde o seu início e sem a possibilidade de qualquer convalidação dos atos instrutórios, motivando, expressamente, a admissibilidade da prova ilícita:

> Assim, diante do conjunto de evidências exposto na inicial — agora corroborado pela admissão feita pelo ex-juiz Sérgio Moro, no bojo do Inquérito 4.831/DF, de que seus dados eletrônicos foram "hackeados"-, reputo não

---

[423] STF, HC 164.493/PR, 2ª Turma. Julgado em: 09/03/2021. **DJe**, 04 jun. /2021. Relator: Min Edson Fachin. Relator do Acórdão Min. Gilmar Mendes.

[424] STF, Plenário, HC 193.726/PR. Relator: Min Edson Fachin. Relator do Acórdão Min. Gilmar Mendes j. em 23/06/2021. **DJe**, 01 set. 2021.

[425] BRASIL. Supremo Tribunal Federal. Habeas Corpus 164.493. Relator: Min. Edson Fachin. Disponível em: https://www.conjur.com.br/dl/gilmar-lewandowski-votam-considerar1.pdf. Acesso em: 05 nov. 2022.

[426] "**Invasão de dispositivo informático.** Art. 154-A. [...] § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa." (Código Penal. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 02 nov. 2022).

[427] STF, PET 8290, de relatoria do Min. Ricardo Lewandowski, em andamento, sob segredo de justiça. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5737419. Acesso em: 02 nov. 2022.

> existirem maiores dúvidas sobre a fidedignidade do teor das mensagens divulgadas pela mídia, embora ilicitamente captadas. (p. 27).

Segue, em capítulo posterior a esta citação, intitulado "IV – ADMISSIBILIDADE DE PROVAS ILÍCITAS" (p. 27 e seguintes), motivando que: **a)** o STF admite o emprego de provas ilícitas no processo penal em benefício do acusado em razão do direito à ampla defesa e à presunção de inocência, citando o RE 583.937/RJ (gravação ambiental por um dos interlocutores); **b)** dentre outros autores, embasa-se na doutrina do renomado processualista penal Eugênio Pacelli, que defende esta possibilidade, com a citação do seguinte ponto:

> a) a violação de direitos na busca da prova de inocência poderá ser levada à conta do estado de necessidade, excludente geral da ilicitude (não só penal!); b) o princípio da inadmissibilidade da prova ilícita constitui-se em garantia individual expressa, não podendo ser utilizado contra quem é o seu primitivo e originário titular;

c) num juízo de ponderação (proporcionalidade), no caso concreto (e várias outras constatações de parcialidade que motiva em seu voto), entre a garantia do sigilo do Telegram do magistrado (obtenção de prova ilegal e violação da intimidade, da vida privada) e a prova de sua suspeição, prepondera esta na "balança" em favor dos direitos fundamentais do réu (condenado), sob pena de se privilegiarem distorções e de uma regra absoluta de inadmissibilidade da prova ilícita em acontecimentos de excepcional gravidade.

O Ministro Gilmar Mendes, relator do Acórdão no HC 164.493, ao final do julgamento, fundamentou no sentido da "Desnecessidade de utilização dos diálogos obtidos na Operação Spoofing" para o julgamento, conforme ementa do voto vencedor:

> [...] O debate sobre o uso dessas mensagens toca diretamente na temática das provas ilícitas no processo penal. O Supremo Tribunal Federal já assentou que o interesse de proteção às liberdades do réu pode justificar relativização à ilicitude da prova. Todavia, a conclusão sobre a parcialidade do julgador é aferível tão somente a partir dos fatos narrados na impetração original, sendo desnecessária a valoração dos elementos de prova de origem potencialmente ilícita pela defesa, que nem sequer constam dos autos deste Habeas Corpus.

O aludido relator para o Acórdão passa, então, a examinar o tema da admissibilidade da prova ilícita, com alguns pontos e exemplos pertinentes, inclusive do direito comparado; em destaque, o objetivo de se provar a inocência do acusado

(pró-réu ou de terceiro sem relação direta com a ilicitude da prova), mesmo por prova ilícita produzida por um corréu, ou, em benesse da vítima em estado de legítima defesa; extrai-se do voto[428]:

> [...] no caso Scheichelbauer vs. Áustria, o Tribunal Europeu de Direitos Humanos consignou que a gravação ilícita de um coacusado poderia ser incorporada ao processo penal, tendo em vista o direito de defesa do réu, para sustentar seu álibi. **A doutrina brasileira aceita a possibilidade de utilização de prova ilícita pró-réu, a partir do princípio da proporcionalidade, considerando o direito de defesa.**
> [...]
> Afirma-se que "desde o ponto de vista de a quem beneficia a ilicitude probatória, **a questão central é determinar se a proibição de admissão ou valoração da prova ilícita deveria ter, como única exceção, aqueles casos em que os resultados beneficiem o imputado ou acusado, ou, inclusive, àquele que não tenha tido nenhuma relação com a ilicitude**" (ARMENTA DEU, Teresa. **A prova ilícita**. Marcial Pons, 2014. p. 82).
> Isso se justifica também a partir das excludentes de ilicitude, pois "quando o agente, atuando movido por algumas das motivações anteriormente mencionadas (causas de justificação), atinge determinada inviolabilidade alheia **para o fim de obter prova da inocência, sua ou de terceiros, estará afastada a ilicitude** da ação" (PACELLI, Eugênio. **Curso de processo penal**. 22. ed. Atlas, 2018. p. 379).
> De modo semelhante, deve-se citar a doutrina do Min. Alexandre de Moraes, que também afirma a legitimidade da prova produzida em "**legítima defesa** de seus direitos humanos fundamentais, que estavam sendo ameaçados ou lesionados em face de condutas anteriormente ilícitas" (MORAES, Alexandre de. **Direito constitucional**. 32ª ed. Atlas, 2016. p. 123).
> Portanto, os elementos de informação aqui analisados poderiam até mesmo ser plenamente admissíveis **em sentido favorável ao réu** no processo penal. (Grifos nossos).

Conclui-se, destarte, haver a limitação da admissibilidade das provas ilícitas, com as ressalvas acima já delimitadas quanto ao caso em concreto. Não se motivou no Acórdão, em nenhum momento, da admissibilidade em favor da Acusação, pelo contrário, criticou o Ministro Gilmar Mendes o anteprojeto de lei das chamadas "10 Medidas Contra a Corrupção", de origem do MPF[429], o qual pretendia alterar o art. 157 do CPP[430], dada sua relativização exacerbada de algo que seria em favor de se evitar abusos no exercício do poder punitivo estatal, em especial:

> Art. 157. São inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação de direitos e garantias constitucionais ou legais.

---

[428] HC 164493/PR, p. 146-148.

[429] BRASIL. Câmara dos Deputados. Anteprojeto de Lei. Disponível em: https://dezmedidas.mpf.mp.br/apresentacao/conheca-as-medidas/docs/medida_7_versao-2015-06-25.pdf. Acesso em: 02 nov. 2022.

[430] Hoje em trâmite na Câmara dos Deputados: Projeto de Lei n. 3.855/2019. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2080604. Acesso em: 02 nov. 2022.

> [...]
> § 2º **Exclui-se a ilicitude da prova** quando:
> [...]
> VII – **usada pela acusação** com o propósito exclusivo de refutar álibi, fazer contraprova de fato inverídico deduzido pela defesa ou demonstrar a falsidade ou inidoneidade de prova por ela produzida, **não podendo, contudo, servir para demonstrar culpa ou agravar a pena**; (Grifo nosso)

Logo, nem a Suprema Corte, a doutrina, ou tampouco o Legislativo, trazem hipótese de admissibilidade de prova ilícita em favor da Acusação para a formação de culpa. A ressalva encontrada na jurisprudência do STF, citada no voto acima, é da possibilidade em nome da legítima defesa da vítima[431]; ou as teses de uso quando em estado de necessidade, ou ainda, por inexigibilidade de conduta diversa para parte da doutrina[432].

Veja-se que, com a abrangência do aceite do *hacking online* ilegal, por particulares, inclusive sob pena de incidirem em crime previsto em lei, apesar de em benefício da Defesa[433] (prova de inocência), gera precedente perigosíssimo, já que pode transformar a exceção em regra que afronta o direito constitucional ao sigilo das comunicações e da reserva jurisdicional. E, diante disso, acertada a motivação do voto vencedor do Acórdão (STF, HC 164493) supra citado em termos mais restritivos à admissibilidade da prova ilícita[434] àqueles relativos ao voto do eminente Ministro Ricardo Lewandowski.

Por fim, cabe relembrar a advertência de que, diversamente do ordenamento jurídico norte-americano, no qual a prova é reputada ilegal somente se produzida diretamente pelo agente público (v.g. o policial), não por particular[435], no Brasil, a regra da inadmissibilidade da prova obtida por meio ilícito visa ao resguardo de direitos e

---

[431] "Utilização de gravação de conversa telefônica feita por terceiro com a autorização de um dos interlocutores sem o conhecimento do outro quando há, para essa utilização, excludente da antijuridicidade. - Afastada a ilicitude de tal conduta - a de, por legítima defesa, fazer gravar e divulgar conversa telefônica ainda que não haja o conhecimento do terceiro que está praticando crime [...]." (STF, HC 74678, 1ª Turma, relator Min. Moreira Alves, publicado em 15 ago. 1997).

[432] ALVES, Leonardo Barreto Moreira. **Processo Penal**: parte geral. 12. ed. São Paulo: Juspodivm, 2022, p. 45.

[433] Lembrando a redação do art. 13 do Projeto do novo CPP, com a possibilidade da investigação criminal defensiva pelo causídico para "tomar a iniciativa de identificar fontes de prova em favor de sua defesa, podendo inclusive entrevistar pessoas" (Câmara dos Deputados. Projeto n. 8045/2010. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1638152&filename=PL+8045/2010. Acesso em: 03 nov. 2022).

[434] HC 164493/PR, p. 146: "[...] de modo a se afastar qualquer eventual discussão sobre o tema da possibilidade de utilização da prova potencialmente ilícita pela defesa".

[435] Conforme rodapé n. 208.

garantias fundamentais, e, por essa razão, "pouco importa quem tenha sido o agente responsável pela produção da prova ilícita – em ambos os casos a prova deve ser considerada ilícita".[436]

Em seu voto no caso penal acima aludido (STF), o hoje aposentado Ministro Marco Aurélio Mello salientou que "Dizer-se que a suspeição está revelada em gravações espúrias é admitir que ato ilícito produza efeitos, valendo notar que a autenticidade das gravações não foi elucidada."[437]

De igual maneira, o Ministro Roberto Barroso, em sessão, pronunciou-se da seguinte forma[438]:

> [...] prova ilícita, produto de crime é prova ilícita. E **sua utilização, sobretudo para fins de sanção a quem quer que seja, é expressamente vedada pela Constituição**. Ademais, trata-se de material sem autenticidade comprovada. Aliás, **na única vez que um desses hackeadores se referiu a mim, disse que eu orientava os procuradores dos processos Lava Jato. Jamais, em tempo algum, isso aconteceu. É simplesmente falso, é a prática contemporânea das *fake news*,** do uso da mentira para atacar quem interfere com os interesses de criminosos. Aliás, faço uma vez mais um registro, com grande correção e dignidade, **o próprio advogado do paciente, que teve acesso às mensagens, desmentiu esse fato**. (Grifo nosso).

De igual maneira, esse mesmo *hacking* ilegal efetuado por particulares (criminosos) de mensagens digitais para favorecer a formação de culpa dos réus pela Acusação, portanto, sem autorização judicial, ausente previsão legal detalhada quanto aos métodos utilizados, talvez desobedecida a cadeia de custódia (até porque há a possibilidade técnica de inserção de conversas no grupo de mensageria digital pelo *hacker*), para todo e qualquer delito, ocasionaria uma burla a tais garantias e direitos constitucionais e a decorrente ilicitude das provas obtidas; na realidade, uma ineficiência na persecução penal.

O professor Dr. Gustavo Badaró levanta tópico que corrobora tal posicionamento[439]:

---

[436] LIMA, Renato Brasileiro de. Manual de processo penal. 11. ed. São Paulo: JusPodivm, 2022, p. 610.
[437] STF, Voto-vista do Min. Marco Aurélio Mello, Segundo Agr. Reg. no HC 193.726, p. 6. Disponível em: https://www.conjur.com.br/dl/marco-aurelio-lula.pdf. Acesso em: 03 nov. 2022.
[438] STF, declaração de voto do Min. Roberto Barroso, Segundo Agr. Reg. no HC 193.726, p. 108. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=757652171. Acesso em: 03 nov. 2022.
[439] BADARÓ, Gustavo Henrique. **Processo Penal**. 10. ed. São Paulo: Thomson Reuters Brasil, 2022, p. 461.

> Poder-se-ia imaginar que a vedação da utilização da prova ilícita representa uma indevida limitação à busca da verdade material e ao próprio livre convencimento do juiz. Todavia [...] **a própria busca da verdade não é ilimitada e não representa um fim que possa ser atingido a qualquer custo.** No processo e, principalmente, na atividade probatória, os fins são tão importantes quanto aos meios. (Grifo nosso)

Resta, assim, acertada a delimitação pormenorizada por lei do *hacking online* estatal de mensagens digitais, por autorização judicial[440], a exemplo da legislação da Alemanha, como exceção permitida dentro do preceito do art. 5º, XII, parte final, da Constituição Federal ("[...] 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;"), ainda pendente de julgamento na Suprema Corte desse país, mas com larga utilização por toda a Alemanha. Só assim a exceção não virará regra, burlando-se a força normativa[441] da Constituição.

4.4.3 Projeto de Lei n. 1515/2022[442]: a chamada LGPD – PENAL

Como projeto legislativo final a ser analisado por novo subcapítulo, porquê diferenciado de todos os demais, imperioso retratar o Projeto de lei n. 1515/2022, conhecido por "LGPD – PENAL" (LGPDP), e, intitulado no projeto como Lei de Proteção de Dados Pessoais[443] para fins exclusivos de segurança do Estado, de

---

[440] Sob pena do crime do art. 25 da Lei de Abuso de Autoridade: "**Art. 25.** Proceder à obtenção de prova, em procedimento de investigação ou fiscalização, por meio manifestamente ilícito: Pena - detenção, de 1 (um) a 4 (quatro) anos, e multa. **Parágrafo único.** Incorre na mesma pena quem faz uso de prova, em desfavor do investigado ou fiscalizado, com prévio conhecimento de sua ilicitude" (Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13869.htm. Acesso em: 03 nov. 2022.

[441] HESSE, Konrad. **A força normativa da Constituição**. Tradução: Gilmar Mendes. Porto Alegre: S. A. Fabris, 1991, p. 27: "[...] o Direito Constitucional deve explicitar as condições sob as quais as normas constitucionais podem adquirir a maior eficácia possível, propiciando, assim, o desenvolvimento da dogmática e da interpretação constitucional. Portanto, compete ao Direito Constitucional realçar, despertar e preservar a vontade de Constituição [...] sua força normativa."

[442] BRASIL. Projeto de Lei n. 1515, de 2022. Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2182274&filename=PL+1515/2022. Acesso em: 05 nov. 2022.

[443] A vigente LGPD (Lei Geral de Proteção de Dados Pessoais) traz conceitos sobre diversas espécies de dados pessoais, cujos conceitos podem ser obtidos no site do Ministério da Cidadania. In: BRASIL. Ministério da Cidadania. **Classificação dos Dados**. Brasília, 30 abr. 2021. Disponível em: https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd/classificacao-dos-dados. Acesso em: 05 nov. 2022.

defesa nacional, de segurança pública, e de investigação e repressão de infrações penais, previstas no art. 4º, III, da vigente LGPD.

Uma interpretação sistemática dos objetivos e fundamentos que elencam os arts. 1º e 2º do Projeto da LGPDP já se observa visar tratamento genérico, sem prejuízo de leis específicas, baseado em direitos e garantias fundamentais que abarcam tanto o direito à privacidade (à intimidade, à liberdade de expressão etc.), quanto à segurança pública, no combate aos crimes (repetida a ideia em seu art. 23), justamente, o conflito de direitos e garantias fundamentais retratado desde o início desta dissertação, fenômeno mundial, especialmente quanto à E2EE em serviços de mensageria digital[444]. Mas, em suma, não se excluem tais direitos e garantias fundamentais, abrindo a possibilidade de uma convivência de possibilidades, o que confirma a tese pacificada de que não são absolutos, sofrendo recortes de forma legítima, obedecido o devido processo legal diante do caso concreto.

Vale frisar o art. 2º, IV, ao dispor que há

> o dever estatal de eficiência nas atividades de segurança do Estado e de defesa nacional e de garantia do direito à segurança pública, por meio da instituição de mecanismos que otimizem a prevenção, investigação e repressão de infrações penais.

Esse preceito traz à tona tanto a questão norte-americana das "circunstâncias exigentes" (art. 3º, inciso II — quanto ao conceito de segurança do Estado[445] — e inciso III — em face do que dispõe de defesa nacional[446] -, do Projeto da LGPDP; vide ainda: arts. 7º e 8º), como exceções extraordinárias à 4ª emenda (hipóteses de dispensa de autorização judicial a serem verificadas no caso concreto), quanto ao argumento da "capacidade de funcionamento da justiça penal (*Funktionstüchtigkeit der Strafrechtspflege*)" do ordenamento jurídico da Alemanha retratado no subcapítulo 3.3, além do princípio da supremacia do interesse público sobre o particular do art. 4º, VII, do Projeto da LGPDP.

---

[444] Daí a crítica ao Projeto da LGPDP pelo Profº. Dr. Luís Greco: falta regulação sobre a obtenção de dados, algo imperativo à autodeterminação informativa, como na Alemanha. Cf.: ESMPU. **Especialistas discutem anteprojeto da LGPD Penal**. Brasília, 15 jan. 2021. Disponível em: https://escola.mpu.mp.br/a-escola/comunicacao/noticias/especialistas-discutem-anteprojeto-da-lgpd-penal. Acesso em: 24 nov. 2022.

[445] "II - atividade de segurança do Estado: toda e qualquer atividade que vise à preservação do território, das instituições, do povo e da soberania nacionais."

[446] "III - atividade de defesa nacional: é a atividade exercida, com ênfase na expressão militar, para a defesa do território, da soberania e dos interesses nacionais contra ameaças preponderantemente externas, potenciais ou manifestas."

É preciso deixar claro que não se afasta a tutela da segurança pública pelas autoridades policiais do art. 144 da Constituição Federal e a investigação e repressão de infrações penais comuns (art. 3º, IV e V, do Projeto da LGPDP; vide ainda o art. 9º).

Essa sistemática inicial do Projeto da LGPDP traz como consequência uma limitação inédita do ponto de vista legal quanto a um diferente tratamento em se tratando do investigado e dos atos resguardados (defesa nacional e segurança do Estado), abarcando a vítima como tutelada dos direitos a seus dados pessoais (art. 5º).

Os artigos 14 e seguintes dessa proposta apontam generalidades quanto ao tratamento e compartilhamento de dados pessoais em atividades de investigação e repressão de infrações penais, dos quais se conclui uma previsão de cooperação entre diferentes órgãos e entidades da Administração Pública e, outrossim, de empresas privadas (arts. 11 e 12 do Projeto). De igual modo se verificou no direito comparado essa tendência, com a observação da previsão legal em todas as hipóteses, em destaque a processual penal, diferenciando-se nos arts. 18 e 19 do Projeto da LGPDP do acesso a dados cadastrais (metadados; como no subcapítulo 4.4.2.5) e os resguardados sob sigilo (casos de interceptação telefônica e telemática).

Nos arts. 41 e seguintes do Projeto da LGPDP segue-se outra convergência, corroborada pela aderência da Convenção de Budapeste pelo Brasil: uma crescente cooperação jurídica internacional em casos de transferência de dados pessoais para outro país ou para uma organização internacional no que tange a atividades de segurança do Estado, de defesa nacional, de segurança pública ou de persecução penal, observados os requisitos do Projeto (arts. 46 e 47) e de leis extravagantes, em especial, garantias ao respeito aos dados do país requerente pela autoridade competente do destinatário, pressupondo o de Estado parte da Convenção do Conselho da Europa, ou, de que o Brasil faça parte, como a Convenção de Budapeste (art. 43). A finalidade é a efetiva cooperação mútua material e de troca de informações técnicas de toda ordem, como a legislativa, doutrinária, por debates práticos etc. (art. 46).

Frise-se que tais garantias de transferência de dados pessoais a outra Nação podem ser dispensadas (art. 44) em casos de extrema gravidade, como na prevenção de ameaça imediata e grave contra a segurança pública no Brasil ou em país estrangeiro, pelo que se denota a imprescindibilidade de exceções, sem prejuízo de

um contraditório diferido, bem como, de um juízo de ponderação, logo, no caso em concreto, expresso no art. 44, § 1º:

> Ainda que se verifiquem os fundamentos previstos no inciso IV[447], os dados pessoais não serão transferidos se a autoridade competente para proceder à transferência considerar que os direitos, liberdades e garantias fundamentais do titular dos dados em causa prevalecem sobre as finalidades que motivariam a transferência por interesse público.

O Projeto da LGPDP prevê, por fim, nos arts. 52 e 53, em casos de infrações às suas disposições, o cabimento de responsabilidade administrativa, sem prejuízo da civil (reparação de danos) e da criminal (mas, nesta, apenas de forma genérica), avançando em pormenorizar penas administrativas, com referência à Lei de Improbidade Administrativa a depender do caso. Revela-se, destarte, mais uma vez, a tendência do legislador brasileiro de não criminalizar as condutas às pessoas jurídicas de direito privado responsáveis por eventuais dados pessoais tutelados pela LGPD e pela proposta da LGPDP.

---

[447] Ar. 44, inciso IV: "para exercer direitos de defesa do Estado no âmbito de processo judicial ou administrativo punitivo."

5 CONCLUSÃO

A criptografia ponta a ponta (E2EE), disponível em diversos serviços de mensagens digitais, é, via de regra, possível de leitura somente entre os seus interlocutores, usuários diretos de cada máquina (v.g. computador e *smartphone*). Há exceções, portanto, mediante o uso de meios alternativos (*backdoors*, *hacking* estatal, infiltração, penetração, *man-in-the-midle* e a própria busca e apreensão do aparelho). Descobriu-se, outrossim, a estratégia da obtenção de inúmeros arquivos para descriptografia por tecnologia futura, como a computação quântica.

Através das tecnologias dispostas atualmente, porém, tais atos investigativos alternativos demandam difícil captação, além do maior custo financeiro e temporal, resultando em ineficiência. Muitas ações criminosas acabam se perdendo da devida persecução penal. Não é algo realizável por simples ofício dirigido às empresas privadas detentoras da tecnologia, como sempre ocorreu com as interceptações telefônicas, principalmente quando se trata de interceptar as conversas em tempo real, algo relevantíssimo em situações de emergência por risco pessoal da vítima, ou de interesse nacional. Exigem um agir de difícil solução pela polícia ou serviços de inteligência, principalmente em países com estruturas de equipamento e de pessoal deficientes, como o Brasil, produzindo-se provas que sequer se sabe se serão admitidas num futuro processo-crime pela nebulosidade que circunda sua sistematização atual. E, mesmo que deferida a interceptação telemática por decisão judicial dentro do devido processo legal e num estado democrático e constitucional de direito, o Estado não verá cumprida sua decisão sob a alegação de impossibilidade técnica da empresa responsável.

Por tais razões, a E2EE tornou-se um dilema mundial, já que obsta investigações criminais sob o fundamento de produção de prova impossível, retirando um legítimo e relevante poder constitucional do Estado. Ocorre que tal "impossibilidade" é proposital pelas empresas (no mínimo há omissão), sob a alegação de resguardo de outros fundamentais direitos e garantias fundamentais.

De fato, existentes certas razões aos lados opostos na polêmica discrepância sobre a E2EE ser ou não mantida por diversos países, pois alguma forma de quebra da criptografia nos serviços de mensageria digital gera, em tese, pela tecnologia atual, risco de que a interceptação telemática possa comprometer os direitos constitucionais da intimidade e vida privada, sigilo, devido processo legal e inadmissibilidade de

provas ilícitas de todos os seus outros usuários, diversamente do que ocorria com a interceptação telefônica. Por outro lado, não há direito ao sigilo absoluto, especialmente na seara investigativa criminal, voltada à segurança pública, inclusive em casos de extrema gravidade, como os de segurança nacional. Tanto que se encontrou precedente advindo da Corte Interamericana de Direitos Humanos, o "Caso Escher e Outros vs. Brasil" (julgado em 2009), cujo núcleo relevante de decisão foi a caracterização da fluidez da comunicação telefônica por seguidas inovações da tecnologia, consignando-se, igualmente, que não existe direito absoluto à privacidade dos cidadãos, ressalvado o abuso do Estado (arbitrariedade), cumulada com a exigência de previsão e obediência da lei para a devida interceptação telefônica, necessária e proporcional (por motivação judicial idônea), visando a um fim democrático e legítimo.

O ideal seria a manutenção da criptografia somada à possibilidade de investigação criminal nos aplicativos de mensagens sem risco à segurança digital, até porque, a eliminação da E2EE é impossível, não porque as empresas não conseguem, ou, os governos não possam impô-la de alguma maneira, mas por ser algo utópico diante: a) da facilidade de se utilizar de aplicativos de mensagens que prezam pela clandestinidade proposital (como o Telegram); b) de programas de computador que permitem a criação de mensagem dotada de criptografia; ou c) de serviço clandestino já prestado a criminosos com tal finalidade.

Nota-se que a aceitação e uso de bilhões de pessoas desses serviços de mensageria digital dotada da E2EE elevam o tema a uma importância mundial. A popularidade e utilidade talvez sejam um respaldo moral às *Big Techs* para não haver um ato incisivo do Estado para impor sua exclusão, até porque, ainda que se obtenha o apoio de várias Nações, sempre haverá a possibilidade de burla para aplicativos estabelecidos em outros países, ou, por uma terceira via à margem da legalidade. E isso revela o porquê da busca da cooperação por diálogo iniciado em importantes países com empresas como o Meta (Facebook), Apple e Microsoft. Ocorre que este é só um lado da celeuma, encabeçado pelo Poder Executivo. Há ainda investidas do Poder Legislativo e do Poder Judiciário, com destaque neste trabalho aos Estados Unidos, Reino Unido, Alemanha e Brasil, os quais, na realidade, caminham por soluções semelhantes, apesar de incertas.

Em síntese, mantida a E2EE está resguardada, de forma quase absoluta, a intimidade, a vida privada, a liberdade de informação e de livre manifestação do

pensamento, o sigilo econômico nas transações empresariais e monetárias pelo meio digital. E, nesta realidade, ao mesmo tempo é possível a investigação criminal de dados criptografados ponta a ponta, todavia, somente por soluções ou estratégias policiais alternativas, por falhas atuais do sistema de segurança, ou, por exercício futuro de nova tecnologia, perdendo-se informações investigativas nos casos em que isso não seja possível. Daqui resulta a forte corrente defensora da exclusão da E2EE, ou, a criação de chaves de acesso ao Estado, em nome da segurança pública, algo rechaçado pelas empresas de tecnologia sob a alegação de impossibilidade técnica, ou, de facilitar o ataque por terceiros mal-intencionados a seus usuários.

Surge, assim, tal como estão investindo importantes países, a procura de uma solução intermediária, para evitar a concretização da eliminação inútil da criptografia por empresas lícitas e de renome internacional, em nome do resguardo de uma gama de princípios e garantias constitucionais igualmente relevantes. Talvez a ajuda dessas empresas seja um caminho mais eficaz que a radicalização do desmanche da E2EE no mundo globalizado.

Apesar dessa possibilidade, não se descarta a imposição de responsabilidades civil, administrativa ou criminal das pessoas jurídicas, como se verificou de diversas legislações do direito comparado e brasileira, através da função de garante, atribuindo-lhes função valorativa do conteúdo de informações as quais, a princípio, são tecnicamente instransponíveis de leitura por estranhos aos interlocutores.

Aliás, a respeito da responsabilidade penal da pessoa jurídica no caso em estudo, há entendimento que repercute tanto na apreciação do direito comparado, quanto, e principalmente, com vistas às possibilidades legislativas no Brasil. Concluiu-se, em suma, que: a) as sociedades podem, em tese, delinquir, tal como realizado na proposta legislativa norte-americana e britânica, além de uma previsão geral na Convenção de Budapeste, porque tais empresas têm a possibilidade de afetar bens jurídicos essenciais ao não agir no caso da interceptação telemática autorizada judicialmente, por um dever legal imposto às empresas privadas detentoras da tecnologia da E2EE, apesar do impeditivo tecnológico atual; b) com o respeito às peculiaridades do ordenamento jurídico de cada país previsto na Convenção de Budapeste, como a preponderância da sanção administrativa no ordenamento jurídico alemão e também prevista nesta Convenção internacional (art. 20), no Brasil é cabível, em tese, a responsabilidade penal das pessoas jurídicas na violação, caso possível

tecnologicamente, deste dever de cooperação com o Estado na interceptação telemática, porquanto o rol de crimes aptos de se sancionar as empresas, previstos na nossa Constituição Federal, é meramente exemplificativo; c) por ora, no Brasil, não há proibição legal ou judicial para a utilização da E2EE, e, aliada à regramento penal normativo inexistente, impossibilitada está a responsabilidade penal da pessoa jurídica (empresas detentoras dessa tecnologia) pela desobediência à determinação judicial de fornecer a interceptação telemática em tempo real de uma conversa de mensageria digital criptografada ponta a ponta.

Veja-se que a prova digital dotada de tecnologia incapaz de conhecimento por terceiros torna, para estes, uma ação inexistente, um sem sentido, ausente a linguagem como conhecimento à produção de um significado para terceiros que não fazem parte desta ação comunicativa, no caso, o Estado, representado pelos agentes de persecução penal legitimamente constituídos para o exercício desta função de controle na prática de crimes. Essa crise na produção da prova penal digital, e, a consequente pressão de várias Nações sobre as *Big Techs* pela quebra da criptografia por algum meio alternativo, está justificada por uma questão universal do ponto de vista não só do Direito, portanto, mas também, da filosofia da linguagem, em especial, na reunião de diversos pensadores da *teoria da ação significativa*, dado o sentido da ação (existente para terceiros conhecerem o contexto de sua realização) advir da interação social, porém, intercedida por regras. Estas, no caso, voltadas a um interesse constitucionalmente legítimo e inerente à defesa dos direitos e garantias fundamentais, criando uma regra de exclusão da intervenção penal estatal pela prova impossível e a irresponsabilidade penal da pessoa jurídica.

Consequentemente, a responsabilidade penal da pessoa jurídica dos provedores desses serviços de mensageria eletrônica criptografados, tal como pretende legislar os EUA, é uma resposta, ao menos formalmente, legítima, democrática, a uma situação inédita de um processo de ausência de conhecimento possível pelo Estado de fatos penalmente relevantes, por conta de uma evolução tecnológica nas mãos do setor privado. Nos projetos de lei em tramitação no Brasil verificados no capítulo 4, contudo, há a ausência de uma concretização efetiva da responsabilidade penal da pessoa jurídica, não passando de previsões genéricas inaplicáveis na prática, restando apenas, por ora, a pretensa imposição de sanções de natureza civil e administrativa.

A interação universal decorrente de uma afim tecnologia de segurança de mensagens em plataformas digitais trazem à tona de forma mais evidente dois fenômenos que irão embasar um novo atuar dos operadores do direito: a) a tendência a um sistema jurídico único, globalizado (ou o mais perto disso possível), no Brasil em especial através da Convenção de Budapeste (aderido por nós e em mais 62 países), tratado internacional de direito penal e processual penal para definir alguns crimes cibernéticos e as formas de persecução penal probatória, inclusive quanto às comunicações de fluxo de dados pela internet (interceptação telemática); b) e o estabelecimento de um modelo de "proceduralização" do direito em face da necessária cooperação ao Estado pelas empresas de tecnologia que fornecem a estrutura necessária para algum controle e produção das provas penais digitais. E ainda assim, porém, resta alternativa outra, como a independência do setor privado à produção da prova, como nas lições sobre o *hacking* estatal na atual situação normativa na Alemanha.

Enfim, essas constatações acima são o indicativo de uma necessária integração mundial de argumentos e conclusões técnicas e jurídicas, evitando-se a incoerência lógica-normativa, pois decorrem de questões universalizadas e de igual origem fática. E a parcialidade dos argumentos a favor e contra a manutenção da E2EE aponta a dificuldade em se estabelecerem verdades básicas para um correto julgamento, notadamente no ramo da tecnologia. O estudo do direito norte-americano, britânico, alemão e brasileiro trouxeram a comprovação dessas conclusões.

Nos EUA, revelou-se, além do debate doutrinário e governamental quanto à ponderação de princípios no plano abstrato e da mutação constitucional da 4ª emenda pela sua Suprema Corte em face da aplicação implícita da Teoria do Mosaico, um Poder Legislativo que já vem atuando para responsabilizar as empresas de tecnologia pelos serviços de mensageria dotados de criptografia ponta a ponta, pressionando-as a encontrar alternativas para uma cooperação ao intuito legítimo de investigação criminal, pois as *Big Techs* sabem que em solo americano o cumprimento de decisão judicial será imperativo.

A partir do caso Jones *v.* United States (2012) passou a Suprema Corte norte-americana a considerar a adormecida Teoria do Mosaico, surgida na década de 70 na Alemanha, seguida da Espanha, quando não se tinha sequer ideia da revolução tecnológica que a internet proporcionou. A Corte máxima dos EUA, ainda aqui implicitamente, em face das novas tecnologias, acrescentou algo de novo quanto ao

alcance da 4ª emenda, criando interpretação mais abrangente que o juízo anterior do que se pode esperar por análise limitada à "expectativa razoável de privacidade" (o chamado "teste de *Katz*"), pelo acesso quase que integral à vida dos cidadãos norte-americanos ao se ter acesso ao *smartphone* (ou outros meios tecnológicos de possível extensa vigilância da vida privada).

A denominada Teoria do Mosaico considera a soma de informações privadas (tais como as peças formadoras de um mosaico) obtidas do cidadão com a visão de seu todo reunido, não de forma isolada de cada elemento. Desse modo, verifica-se, no caso em concreto, se cabível a aplicação dos ditames da 4ª emenda.

Com essa nova linha de raciocínio houve um incremento do que se tinha anteriormente como delineado na proteção constitucional da 4ª emenda, uma mutação constitucional, com consequências jurídicas muito discutidas por seus juízes, principalmente a necessidade e, como visto, sua posterior efetiva concretização, de um atuar do Poder Legislativo para a melhor disciplina dessa trama, evitando-se surpresa probatória a todas as partes envolvidas, que comumente resulta em buscas e apreensões ilícitas, prisões arbitrárias, abuso de poder e, consequentemente, a inefetividade da justiça penal por posteriores anulações de julgamentos. A análise sob a Teoria do Mosaico repetiu-se nos precedentes seguintes julgados pela Suprema Corte dos EUA: Riley *v.* Califórnia (2014) e Carpenter v. United States (2018).

Logo, com o uso da Teoria do Mosaico, o exame do caso sob a égide da 4ª emenda não se limita mais ao que se fazia há décadas, ao se utilizar somente do teste de Katz e da mera análise individual (de forma isolada) e sequencial de cada um dos atos investigados. Dessa nova ótica, porém, somada a situações diferenciadas a depender do tipo de tecnologia utilizada na investigaçao criminal, resultou em precedentes judiciais nas instâncias inferiores dos EUA divergentes, mas, pacificando-se o entendimento da necessária regulamentação legal pelos estados norte-americanos, como enfatizado pelo juiz Alito no julgamento do caso Jones, e pela doutrina, ao enaltecer as garantias da 4ª emenda e defender, para a eficiente investigação policial, a necessária criação de normas prévias às buscas e apreensões para controle de atos ilegais, auxiliando também o Judiciário na proteção constitucional. Como consequência, há recente legislação em vigor, a HB 57/2019, do estado de Utah, tratando dessa nova realidade.

No caso Riley *v.* Califórnia (2014), seguindo esse raciocínio do uso da Teoria do Mosaico, quando se decidiu que a busca e apreensão, sem mandado judicial, de

conteúdo digital de um telefone celular durante uma prisão, é, via de regra, inconstitucional, apontou-se importante exceção à 4ª emenda, a qual se levanta, repetidamente, na doutrina e jurisprudência norte-americana: as denominadas "circunstâncias exigentes". Abrange este termo casos de perigo iminente, grave e específico a pessoas, ou o desaparecimento de provas, de forma que não se obtenha mandado judicial em tempo hábil, e ainda, situação de defesa da segurança nacional e emergências significativas afins; observada que não é aceita na doutrina e jurisprudência norte-americana a mera alegação em abstrato e genérica de ser o crime grave, tal como a intenção de alguns projetos de lei discutidos ao longo desta dissertação.

Tal ponto de exceção é relevante, até porque já utilizado pela Suprema Corte brasileira o emprego de tal conceito em precedente envolvendo a busca e apreensão domiciliar, ao se fundar na razoabilidade para se crer que seria inexigível mandado judicial no caso de se acreditar na prevenção de dano aos policiais ou terceiros, a destruição de provas relevantes, a fuga de um suspeito, ou, por interpretação aberta, alguma outra consequência que frustre, indevidamente, esforços legítimos de aplicação da lei. Mas não só por isso: as legislações postas e propostas dos EUA e do Brasil, dada a fixação jurisprudencial de suas Cortes Supremas, devem seguir raciocínio similar dessas excepcionalidades.

Observe-se que o julgado em questão (caso Riley) é expresso ao mencionar que não vedou a busca e apreensão por mandado judicial do conteúdo do telefone celular do acusado, fato saliente para demonstrar a ausência de um sigilo inviolável e absoluto, mesmo sob a realidade consciente dos julgadores do conteúdo amplíssimo da esfera de privacidade atual sobre a vida dos cidadãos de um *smartphone*. Aliás, em nenhuma decisão judicial, legislação estrangeira, tampouco dos projetos de lei e das leis vigentes que trataram do objeto principal deste estudo elencaram um dever absoluto de sigilo, mesmo nos votos já proferidos pelo STF nas ADPF 403 e ADI 5527 quanto à E2EE.

Ainda quanto à Teoria do Mosaico, no precedente Carpenter *v.* United States (2018), acresceu-se uma outra forma de sua aplicação: a realizada "em duas etapas" (*two-steps*), diversamente da "em uma etapa" (*one-step*) surgida no caso Jones.

No entender da doutrina, a Teoria do Mosaico em "duas etapas" fornece uma maneira de avaliar esses dados fornecidos pelo instrumento tecnológico utilizado melhor que o de "uma etapa", por considerar o tipo de informação revelada e, em

seguida, aplicar os fatos do caso; além disso, permite que os tribunais fundamentem os motivos que certas informações devem ser protegidas ou não, impedindo a ossificação da doutrina da 4ª emenda no campo da vigilância digital, a qual muda rapidamente. Logo, ao invés de se analisar, de uma só vez, como no caso Jones, todos esses dados do mosaico informativo obtido na investigação dos dados arrecadados, verifica-se, primeiramente, a **natureza** da informação ou dados (**primeira** etapa), ou seja, se tem o **potencial** de, por si só, invadir a esfera razoável de privacidade do acusado com base em fatos específicos do caso concreto, e então, somente passada esta etapa com uma resposta afirmativa, passa-se à **segunda** etapa: o julgador deve verificar se a **quantidade** de dados ou informações agregadas (mosaico) como prova dos autos, **efetivamente**, invadiram a privacidade do investigado de forma desarrazoada.

De qualquer forma, o que se revela da atual conjuntura da Teoria do Mosaico e, se a melhor forma é a de uma ou duas etapas, é que ela já está enraizada no ordenamento jurídico norte-americano, oferecendo vantagens na análise judicial de uma possível verificação de violação da 4ª emenda, pois é mais um instrumento aos tribunais a resolver as disputas judiciais, facilitador da resolução jurídica a futuros desenvolvimentos tecnológicos, talvez imprevisíveis por lei anterior. De mais a mais, é apto a embasar o processo de criação de leis e tratados internacionais de uma forma geral e prévia à questão probatória, quanto à eventual reserva de jurisdição e à interpretação a depender da situação sob julgamento (controle judicial), além de uniformizar a matéria, estruturando o trabalho policial.

Complemente-se que essa tendência normativa não é exclusividade norte-americana, mas o que se verifica também no Reino Unido, na Alemanha e no Brasil. E, de mais a mais, a própria Teoria do Mosaico é uma linha interpretativa possível de ser utilizada no Brasil pelo Poder Judiciário e constar, ainda que implicitamente, na redação de nossas leis processuais penais.

Um alerta negativo merece ser citado, porém, quanto à utilização da Teoria do Mosaico e a forma de exceção à 4ª emenda. É que se identificou o desenlace de uma forma abusiva do governo estadunidense agir para justificar a limitação do acesso público a dados secretos que obtém dos próprios cidadãos norte-americanos, sob o argumento de que os terroristas podem superlativizar elementos que, isoladamente, não são importantes, mas que ao serem agrupados o serão (tal como o Mosaico preconiza), sob a justificativa do Estado de dispensa de mandado judicial

na "luta contra o terror", que ao final, retém informações privadas também sob a perspectiva genérica do sigilo estatal dadas as "circunstâncias exigentes".

Sobre a produção legislativa dos EUA, disciplinadora da 4ª emenda em face das novas tecnologias utilizadas na investigação criminal, fica clara a intenção do uso da bandeira midiática do abuso sexual infantil (v.g. a *EARN IT Act*) para contemplar a quebra da criptografia de alguma maneira possível, principalmente do ponto de vista da imposição da responsabilidade penal das pessoas jurídicas responsáveis pelos serviços de mensageria com tal segurança. Aliás, é a mesma retórica levantada no Reino Unido, quando se defende a imposição da responsabilidade penal das pessoas jurídicas e seus dirigentes no projeto de lei que trata da criptografia ponta a ponta (*Online Safety Bill*) e do defendido pelo representante da polícia federal em audiência pública ocorrida no STF no julgamento das ADPF 403 e ADI 5527.

Em face da própria polarização mundial sobre o antagonismo opinativo à E2EE, verifica-se uma forte atuação política do Executivo e do Legislativo. Em todos os países pesquisados há uma tendência de se legislar sobre a matéria. Assim, o caminho da produção legislativa é uma realidade, inclusive em países que adotam o *common law*, como os EUA e o Reino Unido. Nestes dois países se ataca a criptografia de ponta a ponta para, de diferentes maneiras e ainda que implicitamente em alguns casos previstos, haver sua quebra pelas autoridades, diferenciando-se da lei federal e estaduais vigentes na Alemanha. E, na verdade, uma legalização prévia e detalhada é o que a doutrina e a jurisprudência preconizam como a forma correta, sem prejuízo de nestas normas haver fórmulas gerais, abertas, quanto aos meios técnicos utilizados para esse fim, dada a imprevisibilidade das novas tecnologias a serem desenvolvidas.

Outra crítica relevante ao projeto de lei *EARN IT Act* é que, caso aprovado, pode inviabilizar, ainda que indiretamente, o uso de chaves digitais, como a criptografia ponta a ponta nas comunicações eletrônicas (via WhatsApp, Telegram etc.), por ser imputada conduta ilícita a tais empresas de tecnologia por eventuais omissões na apuração de crimes de pornografia infantil que utilizem suas plataformas digitais como meio material da execução desses delitos. Adrede a isso, imposta tal responsabilização, a doutrina traz óbices a tal projeto legislativo sob o argumento de violação da 1ª e 4ª emendas da Constituição dos EUA, pois contraria a liberdade de expressão (sem a proteção da criptografia há possibilidade de violação de senhas de bilhões de usuários) e demandaria buscas privadas pelas empresas, sem autorização

judicial prévia, e, por isso, inconstitucionais, inclusive com repercussões quanto à ilicitude das provas nos processos-crime, desmoralizando a eficácia da justiça penal.

Inclusive já existe corrente argumentativa de ofensa à 4ª emenda, voltada à futura alegação pela Defesa dos acusados em ações penais, por tese de inconstitucionalidade não por conta de violações de outros direitos e garantias fundamentais do acusado (v.g. a privacidade, o sigilo telefônico), mas porquanto acabaria com a voluntariedade de as plataformas digitais buscarem e denunciarem o material ilegal ligado ao abuso sexual infantil por ato de terceiro (*"Good Samaritan" protection*), entregando-o ao "Centro Nacional para Crianças Desaparecidas e Exploradas". Ora, na forma em vigor no ordenamento jurídico norte-americano, tem-se que a busca pelo particular deve ser equiparada à estatal caso seja realizada a pedido de uma autoridade pública, ou seja, somente seria possível sob o escopo da 4ª emenda, por mandado judicial prévio, ou seja, o ato de busca pela empresa, tal como preconizada na lei proposta, tornará a prova ilícita.

Cabe tal precaução ao legislador brasileiro ao tentar se imputar responsabilidades às plataformas digitais (setor privado) à determinação proativa da procura de material ilegal, sem mandado judicial e de forma prévia aos fatos, em tese, criminosos, e não apenas relatar algo por acaso encontrado, porquanto, por analogia, está pacificado tratar a interceptação telemática de cláusula de reserva jurisdicional.

Diante disso, conclui-se que o debate acirrado que se antevê nas Casas Legislativas e, outrossim, nos tribunais dos EUA, dentro da discussão acerca das garantias da 4ª emenda, é a delimitação da abrangência da cooperação dessas empresas privadas de tecnologia na investigação criminal de usuários em suas bases de dados e, talvez, por isso, o sistema do *hacking* estatal alemão tenha aqui uma vantagem enorme, já que independente de um agir do setor privado.

Da legislação norte-americana já vigente, sobressai-se a do estado de Utah (*Electronic Information or Data Privacy Act* - HB 57/2019), porque é a primeira lei do país que trata do objeto desta pesquisa nos EUA, em consonância ao preconizado pela sua Suprema Corte. E, de sua leitura crítica, surgem muitas possibilidades a se seguirem em futura legislação no Brasil sobre a produção de provas penais digitais, como as disposições que tratam: a) da privacidade de informações ou dados eletrônicos, exigindo que a polícia obtenha um mandado judicial para a busca em e-mails e diversas formas de comunicação eletrônica, não só no aparelho (*smartphone*, computador, *tablet* etc.), mas também, no servidor ("nuvem"); b) das informações

eletrônicas e os dados obtidos sem mandado judicial, os quais serão excluídos da consideração em processos, mas cabíveis exceções prescritas na lei nos casos de o aparelho ser roubado e das “circunstâncias exigentes”; c) das "Informações e dados eletrônicos" preconizados na lei, que foram definidos de maneira mais ampla em relação ao grau de proteção advindo do caso Carpenter, exigindo-se as garantias da 4ª emenda a todos os nossos dados eletrônicos, não só à tecnologia do referido julgado (CSLI), ou, dos dispositivos de uso corpóreo do investigado (*smartphone* e microcomputador, por exemplo), porém, agora inclusive, aos documentos armazenados nos servidores, como o *Dropbox* ou o *Google Drive.*

Por fim, uma outra proposta legislativa em andamento nos EUA, concernente à Lei de Acesso Legal a Dados Criptografados (*Lawful Access to Encrypted Data Act*), trata, especificamente, sobre a criptografia digital nos meios de comunicação de uma forma mais genérica, abrangente, em comparação ao projeto de lei *EARN IT Act*, ao determinar que as empresas de tecnologia garantam a possibilidade de descriptografar, ou decodificar, informações sob a E2EE em seus serviços e produtos (nos aparelhos e nas nuvens) para fornecimento às autoridades responsáveis pela persecução penal, mediante prévio mandado de busca e apreensão do juízo competente, sob a 4ª emenda. Exige-se, e isso é algo que pode ser copiado por outras legislações, a favor ou contra à interceptação telemática nos casos de criptografia ponta a ponta, a individualização do próprio dispositivo objeto da ordem judicial, ou seja, não pode ser genérico, e mais, as informações buscadas, e eventualmente obtidas, devem ser isoladas pelo agente, justo em razão da abrangência de informações que um *smartphone* pode trazer nos dias atuais, tal como nos casos julgados pela Suprema Corte dos EUA sob a Teoria do Mosaico, evitando-se abuso ou excesso na investigação, uma intromissão ao direito à privacidade do cidadão.

Aqui, a justificativa do legislador evidenciou o fato de a E2EE nos meios digitais ser um espaço no qual criminosos atuam quase que sem qualquer possibilidade da devida investigação criminal, mesmo mediante autorização judicial e sob os fundamentos da 4ª emenda, com uma apontada desídia das empresas responsáveis ao não desenvolverem a tecnologia apropriada para alterar essa situação, com indício de assim ser de forma proposital.

Por conta disso, esse projeto de lei disciplina que as informações, instalações e assistência solicitadas a serem fornecidas pelas empresas de tecnologia devem descriptografar, ou decodificar, informações no dispositivo eletrônico, ou informações

eletrônicas armazenadas remotamente e objeto do mandado judicial, demonstrando o rol aberto para a efetividade da medida (neste ponto de forma semelhante à vigente lei de Utah), para de alguma forma fornecer tais informações em um formato inteligível; inclusive, provendo o suporte técnico necessário para garantir a execução eficaz do mandado para os dispositivos eletrônicos particularmente nele descritos.

A questão principal, da quebra da E2EE, levanta consequência óbvia: muitos, mas especialmente os "profissionais" do crime, migrarão a outros aplicativos de mensagens dotados de criptografia ponta a ponta, não sediados em solo norte-americano, como o Telegram. Entretanto, pelos bilhões de usuários dos aplicativos de origem norte-americanos (como o WhatsApp e o Facebook Messenger) e a possibilidade de decodificação dos próprios aparelhos celulares que também trocarão mensagens com esses que se utilizam de serviços estrangeiros, já trará efeitos imediatos à investigação criminal. Uma das estratégias práticas das autoridades é que, aliada a essas novas normativas, os próprios fabricantes podem programar os *smartphones* a não aceitarem o *download* de aplicativos fora de um rol permitido em sua loja virtual, como o Google Play (sistema operacional Android) e a App Store (loja oficial de aplicativos para o sistema operacional iOS e iPadOS da Apple), repercutindo por todo o planeta em grau exponencial, pois obstaculiza o uso de aplicativos fora do rol da legislação, mas somente de empresas estabelecidas e identificadas formalmente, já que a chance de criação de celulares e aplicativos voltados à criminalidade, ou de criação de criptografia em conversas privadas, é uma realidade.

O que se verifica já há certo tempo de todo o repertório de tais leis postas e propostas é uma coalização de tendências normativas, isto é, nos EUA de aumento de produção legislativa e, no Brasil, da imposição da vinculação jurisprudencial; e isso é algo positivo à coerência fática-normativa apta ao desenvolvimento da cooperação jurídica internacional probatória, notadamente concretizada na Convenção de Budapeste.

No Reino Unido, o projeto de lei conhecido como *Online Safety Bill,* assim como a normativa posta e proposta dos EUA, pretende impor um dever legal de cuidado a certos provedores de serviços no meio digital para moderar o conteúdo gerado pelo usuário, a fim de que os demais não sejam expostos a ilegalidades (abuso sexual infantil, terrorismo e material suicida), com previsão de multas e penalidades para as pessoas físicas e jurídicas que não cumprirem esse dever, inclusive de natureza criminal, sob o termo *duty of care* ("dever de cuidado") disposto na sua Seção

117. Tal como no criticado projeto de lei norte-americano *EARN IT Act*, as empresas de tecnologia que hospedam conteúdo gerado pelo usuário, ou permitem que as pessoas se comuniquem, serão legalmente obrigadas a identificar, remover e limitar, por ato próprio, a disseminação de conteúdo ilegal, sob pena de multa em até 10% de seu faturamento pelo regulador de danos online, o *Ofcom* (abreviação de *Office of Communications*), agência reguladora de mídia do Reino Unido e prevista no referido projeto de lei como órgão fiscalizador do conteúdo disseminado na internet por tais provedores ou plataformas digitais.

A novidade em destaque do projeto britânico é a de que, para cumprir esse dever legal de cuidado pelos provedores de serviços sob seu escopo foi criado instrumento tecnológico, o qual promete manter a E2EE através do *software* denominado CSS (*client side scanning*, traduzido como: "varredura do lado do cliente"), em *smartphones*, *tablets* e computadores, para realizar a varredura algorítmica de texto, imagens, vídeos e arquivos de conteúdo ilícito antes de ser enviado pelo dispositivo, impedindo que seja remetido e com alerta à polícia, de forma muito semelhante à tecnologia alemã; de igual forma desta, com corrente contrária ao uso da CSS por sua alegada incompatibilidade técnica à manutenção do sigilo pela criptografia, pois abre brechas para intrusão de terceiros maliciosos.

Portanto, repete-se na proposta britânica argumento crítico das propostas legislativas norte-americanas: a única maneira de os provedores de serviços que oferecem criptografia de ponta a ponta cumprirem esse dever de cuidado seria remover ou enfraquecer a criptografia que eles oferecem. E, tal como os projetos de lei dos EUA examinados, a pretensa lei não proíbe a E2EE de forma direta, contudo, as responsabilidades que ela impõe aos provedores de serviços o fazem implicitamente.

Repete-se aqui o problema verificado nas pesquisas bibliográficas do capítulo 2 sobre o WhatsApp e suas falhas técnicas, além daqueles demonstrados nas audiências públicas do STF (ADPF 403 e ADI 5527): a falta de estudo (ou sua comprovação) por perícia imparcial a eventual juízo de valor legislativo ou judicial sobre os meios tecnológicos possíveis utilizados para compatibilizar a segurança da E2EE e a investigação criminal, como o CSS do Reino Unido e o *software* adquirido pela Alemanha. O uso da retórica para um lado ou outro quanto à E2EE não é suficiente, por desencadear mero juízo opinativo no plano abstrato da colidência de princípios constitucionais.

De forma diferenciada, a Alemanha, através de lei já vigente desde 2017, alterou o seu Código de Processo Penal quanto à interceptação telemática para possibilitar a instalação de cavalos de Troia do Estado, além de posteriores legislações estaduais. Já está sacramentado no país o uso desse meio alternativo de investigação criminal para, mantendo a tecnologia da E2EE, possibilitar a busca da prova penal digital. A sua Suprema Corte ainda sequer iniciou o julgamento das ações constitucionais que questionam essa lei, e, se por um lado esta já decidiu que o sigilo das informações desses novos modelos tecnológicos de armazenamento de informação privada não são um direito fundamental absoluto, por outro olhar, a doutrina encara o *software* de espionagem como um método oculto excepcionalíssimo de investigação, pois demasiadamente intrusivo na vida privada do investigado (espionagem em tempo real no fluxo de conversas e amplo acesso a dados do *smartphone*), exigindo detalhamento normativo mais amplo que o da mera interceptação telefônica, algo já delimitado pelo projeto dos EUA chamado *Lawful Access to Encrypted Data Act*, de possível aplicação no Brasil.

Logo, inobstante críticas pela própria natureza divergente quanto à E2EE, esta valorização da "taxatividade" em complemento às regras de interceptação telefônica e telemática já presentes no Código de Processo Penal alemão foi a opção mais acertada, pois ausente regras claras do agir das forças estatais de investigação e a prévia delimitação de regras de procedimento para evitar provas ilícitas ou inviáveis de perícia para a contraprova pela Defesa do investigado resultará, provavelmente, na ineficiente persecução penal e o descrédito da Justiça.

Do estudo de precedentes jurisprudenciais do STJ verificou-se que a interceptação telemática em tempo real via o WhatsApp Web (o "espelhamento" de mensagens), apesar de utilizada em diversos casos pelas autoridades da Alemanha, restou, por ora, decidido no Brasil como prova ilícita, com a observação de que há segredos não divulgados da forma como esses agentes vêm agindo nesse tipo de investigação.

Nesta seara cabe uma advertência: não se deve assentar tal precedente judicial do STJ como uma verdade absoluta a todos os casos, a fim de que não se exclua tal estratégia investigativa e as provas produzidas de forma indiscriminada no ordenamento jurídico brasileiro. Fatores como a obsolescência programada da tecnologia, uma política empresarial parcial e agressiva, a pressão estatal através de ações do Executivo e do Legislativo de diferentes países, além da natural apreciação

artesanal nas decisões judiciais, podem repercutir em visão futura diversa. Além disso, há um espírito de sistematização do regime jurídico universal (na medida do possível) quanto à cooperação jurídica em relação à produção da prova penal digital, sem falar das lições filosóficas da ausência de uma verdade única ou última, em especial pela variável espaço-tempo.

No Brasil, o STF iniciou o julgamento de duas ações constitucionais sobre a situação dos serviços de mensageria digital e a E2EE por ordens de bloqueio judicial do WhatsApp, multas diárias e até prisão de seus representantes, após o descumprimento por parte do aplicativo da realização de interceptação telemática, sanções ora suspensas por nossa Suprema Corte (ADPF 403 e ADI 5527). Ocorre que, o resultado final de mérito dessas demandas, se for pela possibilidade de ser imposta ao WhatsApp alguma forma de ruptura de seu sistema de criptografia ponta a ponta, possivelmente, não será cumprido, conforme precedentes de casos semelhantes de *exequatur* de decisões judiciais estrangeiras nos EUA. E não se pode descartar opções empresariais imprevisíveis para tentar se abster do cumprimento de obrigação de quebra da E2EE, tal como a indisponibilidade de seu serviço no Brasil, já que o sistema operacional do WhatsApp é um só para todo o mundo.

Aliás, do direito comparado e da pesquisa bibliográfica, obtiveram-se dados que rebatem os fundamentos até agora proferidos por seus doutos relatores. No voto da Excelentíssima Ministra Rosa Weber verificou-se, diversamente do que ponderou, que há sim tendência legislativa e de ações governamentais nos EUA, dentre outros países, no sentido de forçar as empresas a criar tecnologia voltada à leitura de mensagens criptografadas, inclusive para a criação de *backdoors*. O ponto controverso, ausente na Lei n. 9296/96, é a determinação da quebra de E2EE às empresas privadas, requisito excluído da lei alemã pela criação de software próprio, mas cuja interpretação, com fulcro no Marco Civil da Internet, é objeto dessas ações constitucionais. E, quanto ao voto do Exmo. Ministro Edson Fachin, verificou-se que a alusão ao argumento estatístico de ausência de prova de uma escalada no uso da E2EE para o cometimento de crimes graves se deu sem base científica oficial, pois não demonstrado seguir critérios matemáticos, não traz dados convincentes em laudo técnico imparcial (com o adendo de o magistrado dever se limitar às provas disponíveis nos autos). Fora isso, tratam esses subsídios técnicos citados de realidades distintas da brasileira, cujo índice de criminalidade, no mínimo, mereceria a ideia em se pesquisar, cientificamente, o tamanho do impacto nas investigações

criminais da possibilidade de interceptação telemática de fluxo de comunicações dotadas de criptografia ponta a ponta em tempo real. Ainda, as estatísticas citadas em seu voto podem estar mascaradas pelo desconhecido, justamente porquanto objeto de prova impossível pela existência de vítimas veladas (processo de macrovitimização) pela escalada na ocorrência de crimes cibernéticos.

Os projetos de lei dos EUA pretendem, ao contrário desses votos, a imposição, mesmo indireta, de quebra ou fragilização de criptografia ponta a ponta, sob pena de responsabilização cível e criminal das empresas que sejam omissas no combate aos crimes que discriminam. E isso, repita-se, repercute na dificuldade da conciliação de todo o arcabouço jurídico internacional para a efetivação da pretendida cooperação jurídica internacional através da Convenção de Budapeste, até porque, prevalecendo tais entendimentos no STF, ir-se-á de encontro ao núcleo legislativo vigente da Alemanha (permitindo a interceptação telemática de mensagens com a E2EE por "cavalo de Troia" do Estado) e os projetos de lei do Reino Unido e dos EUA.

Veja-se que a questão da responsabilidade civil e criminal das empresas responsáveis pelas mensagens transmitidas e seus conteúdos é outro ponto controvertido, mas que já se debruçou a jurisprudência e o legislador (arts. 18 e 19 do Marco Civil da Internet) em casos análogos, e, contrariamente ao objetivo do *EARN IT Act*, o sentido que se sinaliza é o de afastar a responsabilidade objetiva dessas companhias para o cabimento tão só da subsidiária e subjetiva em caso de "desídia a uma ordem judicial competente", argumento que, em certa medida, o STF está se debruçando nessas ações constitucionais, mormente visando à efetividade da decisão final dos Acórdãos, pois, a criptografia ponta a ponta, por si só, ou seja, afastadas hipóteses excepcionais de meios alternativos de investigação, é inviolável.

Logo, por enquanto, resta em tais hipóteses de mensagens criptografadas a investigação criminal por outros meios probatórios, como o fornecimento de metadados em e-mails, fotos, vídeos, dentre outras informações dispostas em nuvem (Google Drive, Apple iCloud etc.), através de pedidos diretos a tais provedores (art. 13-A do CPP; art. 17-B da Lei 9613/98; art. 15 da Lei 12.850/13) e, judicialmente, por mandados de busca e apreensão de dados armazenados nos servidores (arts. 240 e seguintes do CPP), além da própria interceptação telemática de comunicações digitais em fluxo, quando possível pela tecnologia existente, como especificado no art. 7º, incisos I a III, do Marco Civil da Internet e jurisprudência do STJ.

Permanece, a lacuna legislativa vigente específica quanto à E2EE no Brasil, seguindo a celeuma do direito comparado. Repete-se na análise dos projetos de lei pátrios o argumento da impossibilidade técnica de cumprimento da decisão judicial, isentando as pessoas jurídicas de responsabilidades, seguindo esse entendimento o STJ (RMS n. 60.531/RO).

Desse modo, a realidade brasileira é praticamente a mesma de países como os Estados Unidos, Reino Unido e Alemanha: problemas práticos e jurídicos decorrentes da mesma origem pela identidade no uso de aplicativos e plataformas digitais por bilhões de usuários. Cada Nação com similitudes e diferenças entre si merecem estudo comparativo não só por conta de aprendizado através da troca de tecnologias de investigação, mas de experiências e questionamentos de diferentes frentes (autoridades policiais, Legislativo e Judiciário, universidades etc.) e até possíveis acordos entre o Poder Executivo e o setor privado (*Big Techs*). Tudo isso também em razão de uma crescente necessidade de transnacionalidade na cooperação de provas, o denominado Estado Constitucional Cooperativo, aderindo estes três países e o Brasil à Convenção de Budapeste. Almejam os diversos países estudados, a olhos vistos, estancar falha persecutória penal que vem beneficiando criminosos, sem esquecerem-se das garantias e direitos fundamentais dos cidadãos.

Não por acaso que a Convenção de Budapeste dispõe que se estabeleça, no direito interno de cada Estado Parte, a criação, por lei, de diversos tipos penais para a sua devida implementação, abrangendo a tentativa, coautoria e a responsabilidade penal da pessoa jurídica. E o Brasil está se erguendo, lentamente, a esta nova realidade, inclusive ao eleger, como direito constitucional, a proteção de dados pessoais (inclusive digitais), conforme o art. 5º, LXXIX, da CF (Emenda Constitucional n. 115, de 2022), e tramitar, na Câmara dos Deputados, o Projeto de lei n. 4.939/2020, o qual estabelece princípios e diretrizes à aplicabilidade do Direito da Tecnologia da Informação, além de normas de obtenção e admissibilidade de provas digitais na investigação e no processo e dispor sobre diversos tipos penais, que abrangem os previstos na Convenção de Budapeste, possibilitando sua aplicação em nosso ordenamento jurídico. Também o STF segue esta ideia de facilitação, ou, de desburocratização da colheita da prova, inclusive daquelas produzidas em casos criminais de interceptação telemática por tratado internacional bilateral.

Semelhante a tal projeto legislativo e à Convenção de Budapeste, a lei do *Cloud Act,* vigente desde 2018 nos EUA, é expressa à aplicabilidade do *Stored*

Communications Act para os dados mantidos no exterior por empresas estabelecidas no território norte-americano (mesmo se estiverem os dados armazenados fora do seu território); ademais, cria a possibilidade de acordos executivos que permitem a comunicação direta de solicitações de dados entre os EUA e outros países, em uma via de mão dupla.

Inclusive o STF, na ADC 51, ainda em julgamento, semelhante ao disposto no *Cloud Act*, discute a possibilidade de as autoridades brasileiras solicitarem, diretamente às empresas de tecnologia que ofertem seus serviços no Brasil, dados e comunicações eletrônicas (na forma do art. 11 do MCI e no art. 18 da Convenção de Budapeste), destacando-se dos três votos favoráveis até agora proferidos a ideia de que os arquivos eletrônicos não são exatamente objetos transportados fisicamente de um lugar para o outro, isto é, não faz sentido tratá-los como coisas com pesos e dimensões, que precisem de alguma autoridade no exterior para serem trasladadas até aqui. É exatamente a crítica polêmica de precedente norte-americano *Microsoft Corporation v. United States of America* (2016), quando não se aplicou o *Stored Communications Act* extraterritorialmente, apesar de plenamente possível de acesso pela empresa dentro dos EUA, só pelo fato de estar a prova penal em arquivos digitais localizados no exterior, exigindo-se que os dados armazenados também estejam dentro do território norte-americano.

Pode-se resumir de uma análise geral da Convenção de Budapeste haver intrínseca interlocução do direito penal e processual penal à eficaz tutela dos bens jurídicos protegidos quanto aos crimes cibernéticos, constatação que, apesar de antes já existente, agora é superlativa pela difícil produção de provas digitais nesta nova era tecnológica, notadamente pela E2EE, a diminuta colaboração das empresas de tecnologia, a adaptação legislativa no direito interno e internacional, além da falta de estrutura policial, sem contar os posicionamentos jurisprudenciais naturalmente atrasados em relação aos fatos que já deveriam estar abarcados pelo arcabouço jurídico-normativo.

Todo este arcabouço de informações de diferentes países serviu para comprovar algo só percebido ao final da confecção do capítulo 4 desta dissertação: o processo legislativo do Brasil na seara objeto desta pesquisa científica existe, de uma forma apenas geral, porém, é precário, confuso, desorganizado e atrasado, inclusive quanto à falta de conhecimento do direito comparado e, até mesmo nacional em

muitos pontos, algo fundamental no aprendizado de erros e acertos de questões já há tempos, efetivamente, concretizadas noutras Nações.

O legislador, contudo, ainda que ausente nas justificativas do respectivo relator dos projetos de lei examinados, trouxe propostas que indicam a mesma ideia já defendida pelos países estudados. A própria aprovação da Emenda Constitucional n. 115 demonstra que alguns parlamentares já se ativeram à existência de um sistema jurídico voltado à cooperação probatória digital, universalizado na medida do possível, coerente do ponto de vista normativo para a rapidez que o devido processo legal penal exige, tal como evidenciado pela coerência fática dominada pelas grandes empresas de tecnologia. Há sim acertos, novas propostas em consonância com algumas inovações tecnológicas, mas que se arrastam por anos de processo legislativo.

Em vista disso, para uma devida sistematização diante da complexidade e abrangência da matéria quanto aos projetos de lei brasileiros, dividiu-se o subcapítulo 4.4 em três grandes grupos, mirando a normatização da interceptação telemática em casos de criptografia ponta a ponta, mas a esta não se resumindo, por temas imprescindíveis a ela correlacionadas.

Na primeira parte dessa subdivisão houve a análise crítica sobre a Lei n. 9296/96 e as responsabilidades das empresas provedoras do serviço de comunicação diante das novas possibilidades digitais (Projeto de lei n. 5285/2009 e seus apensamentos), chegando-se à conclusão de ausência da figura da responsabilidade penal da pessoa jurídica, apesar da criação de tipo penal voltado ao combate daqueles envolvidos com equipamentos que realizam escuta telefônica e telemática ilegal, inclusive de dados digitais, limitando-se a pessoas físicas; inclusive se imputa o crime a quem utiliza a criptografia para proteger comunicação de voz, imagem e dados, em desacordo com as normas expedidas pelo órgão federal competente (art. 21, caput e parágrafo único, do Projeto de lei n. 5285/2009).

Verificou-se que o Projeto de lei n. 1394/2021 possui uma louvável previsão exemplificativa de métodos tecnológicos para possibilitar a interceptação almejada (art. 9º-A da Lei n. 9.296/96); o Projeto de lei n. 2942/2015 dispõe sobre o contraditório diferido obrigatório ao investigado, semelhante à HB 57/2019 (Utah, EUA); e no Projeto de lei n. 3372/2021 indica-se, expressamente, o "espelhamento" como meio de obtenção da prova digital, apesar do atual posicionamento do STJ quanto ao WhatsApp Web, em contraposição à praticada na Alemanha, aqui sem notícia de qualquer anulação judicial das provas.

Na segunda parte (subcapítulo 4.4.2), colocou-se como gênero os Projetos de lei relativos ao Marco Civil da Internet e à E2EE, legislação que vem se baseando o STF no julgamento das ações constitucionais que tratam da criptografia ponta a ponta (ADPF 403 e ADI 5527). Assim, no Projeto de lei n. 9808/18 propõe-se acrescentar ao art. 10 da Lei n. 12.965/14 os parágrafos 5° e 6º, conferindo poderes de acesso a serviços de mensageria digital privada em casos de flagrância por crime hediondo, de tráfico de drogas ou terrorismo, por fornecimento de chaves de quebra de criptografia pelos provedores diretamente aos delegados de polícia, ferindo a reserva jurisdicional prevista em lei e na Constituição Federal; e também, neste aspecto, o projeto perderá parte de seu objeto por eventual decisão contrária do STF na ADPF 403 e na ADI 5527, podendo ser mantido o projeto quanto ao acesso aos metadados, tal qual destacado no Projeto de lei n. 4442/2019 (neste de acordo inclusive com o caso Jones e a Teoria do Mosaico), o qual se destaca ao prever a responsabilidade criminal dos provedores somente de uma forma genérica, inexequível, portanto.

Já o Projeto de lei n. 6960/2017 está em consonância ao novo alcance da 4ª emenda dos EUA, quanto à abrangência do termo "*effects*", abarcando não só "o computador ou qualquer dispositivo que se conecte à internet" (na redação atual do MCI, art. 5º, II), mas também o dispositivo móvel (celulares, *smartphones*, *tablets* ou similares), ou terminais fixos, que não possibilitem o deslocamento do dispositivo conectados à internet de forma concomitante (art. 7º, III, do MCI); conferindo maior abrangência da tutela constitucional e controle judicial (limitador do poder de polícia).

No Projeto de lei n. 11.007/2018 trata da obtenção de prova penal digital sob o pretexto de atos terroristas digitais (ciberterrorismo), criminalizando a pessoas físicas condutas relacionadas à E2EE; mas, falha ao considerar somente a gravidade em abstrato dos crimes de terrorismo e ao não prever uma fórmula geral, talvez melhor posicionada nas disposições do MCI, quanto às exceções envolvendo as "circunstâncias exigentes".

Seguindo-se na preocupação pelos atos de ciberterrorismo, crimes hediondos e a produção da prova penal digital, verificou-se que no Projeto de lei n. 2418/2019, tal como à luz da legislação alemã, erigiu-se a possibilidade do *hacking* estatal nos sistemas dotados da E2EE, uma substancial alteração da função do provedor com a introdução do art. 21-A do MCI, pois, sob pena de responsabilidade civil, passa a ter função proativa, de fiscalização, independentemente de qualquer notificação da parte interessada, como prevê o vigente art. 21 dessa lei, o qual também dispõe que tal

responsabilidade tem a condicionante da possibilidade técnica de agir da pessoa jurídica (em harmonia ao que se verifica no direito comparado quanto à E2EE), objeto este de crítica dos defensores de um método que possibilite a investigação criminal, porque perpetua uma escusa de interesse empresarial de descumprimento de ordens judiciais pela alegada quebra impossível da criptografia. E, quer-se neste projeto prever duas hipóteses de fiscalização pelo Estado (arts. 21-A e 3º, ambos deste projeto): o das redes públicas de internet (fóruns *online* e redes sociais), e, a interceptação telemática de *smartphones*, dentre outros dispositivos ligados à intimidade das pessoas nas suas conversas telefônicas, ou de mensageria privada digital.

Por fim, importante reflexão advém ao se apreciar o Projeto de lei n. 2419/2022, o qual, apesar de tratar da alteração do art. 8º-A, §4º, da Lei n. 9296/96 (prova obtida da captação ambiental em prol da Defesa e da Acusação), pode repercutir no eventual entendimento do STF sobre a admissibilidade, ou não, do hackeamento legal (feito pelo Estado, como na Alemanha) e ilegal (do caso concreto julgado quanto ao uso de provas obtidas por *hackers* em celulares de magistrados e membros do Ministério Público no aplicativo Telegram; c.f. STF, HC 164493), mormente em face das mensagens dotadas da E2EE.

Neste peculiar ponto, verificou-se que a Suprema Corte, o Legislativo e a doutrina não trazem hipótese de se considerar a prova ilícita em favor da Acusação para a formação de culpa. Caso se aceitasse o *hacking* ilegal, por particulares, mesmo em benefício da Defesa (prova de inocência), geraria precedente perigosíssimo, já que poderia transformar a exceção em regra que afronta o direito constitucional ao sigilo das comunicações e da reserva jurisdicional. E, diante disso, acertada a motivação do STF em termos mais restritivos à admissibilidade da prova ilícita, cabendo relembrar que, no Brasil, a regra da inadmissibilidade da prova obtida por meio ilícito visa ao resguardo de direitos e garantias fundamentais, pouco importando quem tenha sido o responsável pela produção da prova ilícita. Por isso, acertou a reforma processual penal alemã ao delimitar, de forma pormenorizada, o *hacking* estatal de mensagens digitais, por autorização judicial, exemplo que pode ser copiado no Brasil, sem a exceção ao sigilo nas comunicações digitais virar regra, como forma de burla à força normativa da Constituição.

Na terceira e última subdivisão do capítulo 4, coube a verificação do Projeto de lei n. 1515/2022, a chamada Lei Geral de Proteção de Dados Pessoais em matéria

Penal (LGPDP), por encabeçar ideias e conceitos já vigentes embasados na Lei n. 13.709/2018 (LGPD). O projeto visa à segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais, previstas no art. 4º, III, da LGPD.

A primeira conclusão, de uma interpretação sistemática dos objetivos e fundamentos que elencam os arts. 1º e 2º do Projeto da LGPDP, é a de se pretende impor um tratamento genérico dos direitos e garantias fundamentais, que abarcam tanto o direito à privacidade, quanto à segurança pública no combate aos crimes (art. 23), justamente, o conflito de direitos e garantias fundamentais de fenômeno mundial quanto à E2EE em serviços de mensageria digital, ou seja, há uma convivência de possibilidades, o que confirma a tese pacificada de que não são eles direitos absolutos, sofrendo recortes de forma legítima, satisfeito o devido processo legal diante do caso concreto.

No seu art. 2º, IV, é trazida a questão norte-americana das "circunstâncias exigentes" (quanto ao conceito de segurança do Estado e de defesa nacional), tais como as exceções extraordinárias à 4ª emenda, coadunando-se, outrossim, ao fundamento da "capacidade de funcionamento da justiça penal" (*Funktionstüchtigkeit der Strafrechtspflege*) do ordenamento jurídico da Alemanha.

Outros aspectos importantes merecem exposição do projeto da LGPDP: a) a tutela dos direitos envolvidos quanto aos dados pessoais das vítimas (art. 5º), preocupação louvável e esquecida em muitas legislações; b) o compartilhamento de dados pessoais em atividades de investigação e repressão de infrações penais, abrangendo a cooperação de empresas privadas (arts. 11 e 12), em convergência à parte da situação estrangeira; c) a confirmação da necessária lei prévia dispondo de hipóteses para obtenção da prova penal digital, como o acesso a dados cadastrais (metadados) e os resguardados sob sigilo telefônico e telemático (arts. 18 e 19 do Projeto da LGPDP); d) a crescente cooperação jurídica internacional em casos de transferência de dados pessoais para outro país, ou para uma organização internacional, no que tange a atividades de segurança do Estado, de defesa nacional, de segurança pública ou de persecução penal, observados os requisitos do Projeto (arts. 41, 43, 46 e 47) e de leis extravagantes, sobressaindo agora em face dos ditames da Convenção de Budapeste; e) prevê-se (arts. 52 e 53) a possibilidade da responsabilidade administrativa, civil (reparação de danos) e criminal (mas, nesta, apenas de forma genérica), evidenciado o direcionamento do legislador brasileiro em

não criminalizar as condutas às pessoas jurídicas de direito privado responsáveis por eventuais dados pessoais tutelados pela LGPD e pela proposta da LGPDP.

Como conclusão geral do exposto, em razão de toda a releitura crítica desses projetos de lei, ponto relevante é a demonstração de que a base da pesquisa científica com supedâneo na experiência estrangeira é fundamental e inexorável à criação do processo legislativo quanto à E2EE e todo o seu entorno, restando comprovada a capacidade do uso do direito comparado funcionalista na busca de soluções a problemas globais, como o das novas tecnologias digitais à investigação criminal.

No Brasil, aliás, infelizmente não se verificou projeto de lei em fase avançada de aprovação para a resolução desse problema em discussão por todo o mundo, especificamente, quanto à interceptação telemática de mensagens digitais protegidas pela criptografia ponta a ponta, não obstante restar pacificado por todos os países pesquisados a normatividade como a solução acertada nessas questões investigativas criminais, relegando ao Poder Judiciário (STF; ADPF 403 e ADI 5527) função que por todo o mundo parte (e assim se recomenda) do Poder Legislativo. Neste sentido, quanto à E2EE, temos projetos esparsos e conflitantes a experiências externas mais acertadas, revelando severo atraso normativo, apesar da adesão do Brasil à Convenção de Budapeste e o julgamento da questão por nossa Suprema Corte.

A presente dissertação revelou que nada é definitivo a respeito de seu objeto principal: a produção e a admissibilidade da prova penal digital, sobretudo quanto à E2EE. Diga-se isso, não por um clichê argumentativo, mas pelas inovações constantes da tecnologia ordenar uma nova postura analítica ainda recente e discrepante à velocidade quando comparadas aos poderes do Estado. Por ser algo muito recente, dependente de uma interpretação global ainda tentando se estabelecer e se organizar, resta caminhar da maneira como exposta ao longo deste estudo, utilizando-se da apreciação do direito comparado como algo inerente ao exercício metodológico, adaptando-o ao ordenamento jurídico interno enquanto viável e útil à resolução dos conflitos de cada Nação no âmbito criminal. E por tal motivação, deve ser lembrada a advertência doutrinária sobre o perigo dos precedentes inflexíveis de exclusão das provas produzidas e, por conseguinte, a relevância de uma nova lei formal, geral e abstrata, quanto ao controle epistêmico na produção e admissibilidade da prova digital penal no direito brasileiro, tal como preconizado pela Suprema Corte norte-americana no caso *Jones v. United States*, e, como já solidificado na Alemanha.

REFERÊNCIAS

ABBOUD, Georges; CAMPOS, Ricardo. A autorregulação regulada como modelo do Direito proceduralizado. In: ABBOUD, Georges; NERY JR., Nelson; CAMPOS, Ricardo (Org.). **Fake news e regulação**. 3. ed. São Paulo: Thomson Reuters Reuters Brasil, 2021. p. 131-151.

ACADEMY BINANCE. **O que é criptografia de ponta a ponta (E2EE)?** Jul. 2020. Disponível em: https://academy.binance.com/pt/articles/what-is-end-to-end-encryption-e2ee. Acesso em: 30 nov. 2021.

ACLU. **NSA spying on americans is illegal**. Disponível em: https://www.aclu.org/other/nsa-spying-americans-illegal. Acesso em: 25 nov. 2021.

AGUIAR, Poliana P. de M.; BRENNAND, Edna G. de Góes. Gestão jurídico-estratégica do cibercrime no contexto da ciberdemocracia. In: BRANT, Cássio (Coord.). **Direito digital & sociedade 4.0**. Belo Horizonte: D'Plácido, 2021. p. 753-780.

AHLAM, Rafita. Apple, the Government, and You: Security and Privacy Implications of the Global Encryption Debate. **Fordham International Law Journal**, v. 44, n. 3, p. 771-846, 2021. Disponível em: https://ir.lawnet.fordham.edu/ilj/vol44/iss3/5. Acesso em: 26 nov. 2021.

ALEXY, Robert. On Balancing and Subsumption. A Structural Comparison. **Ratio Juris**, v. 16, n. 4, p. 443-449, dez. 2003.

ALEXY, Robert. **Teoria dos direitos fundamentais**. Tradução: Virgílio Afonso da Silva. São Paulo: Malheiros, 2008.

ALLE, Saulo Stefanone. Produção probatória e cooperação jurídica internacional em matéria penal. **Revista Brasileira de Ciências Criminais**, São Paulo, v. 156, p. 425-452, jun. 2019.

ALMENARA, Igor. Facebook Messenger e Instagram só terão criptografia de ponta a ponta em 2023. **Canaltech**, 23 nov. 2021. Disponível em: https://canaltech.com.br/redes-sociais/facebook-e-instagram-so-terao-criptografia-de-ponta-a-ponta-em-2023-202585. Acesso em: 29 nov. 2021.

ALVES, Leonardo Barreto Moreira. **Processo Penal**: parte geral. 12. ed. São Paulo, Juspodivm, 2022.

AMSTERDAM, Anthony. G. Perspectives on the Fourth Amendment. **Minnesota Law School**, n. 848, 349-477, 1974. Disponível em: bit.ly/3h5rXba. Acesso em: 20 out. 2021.

ANDRADE, Daiane. Mesmo com novos peritos, PR ainda tem menos de 50% do efetivo previsto em lei. **Gazeta do Povo**, Curitiba, 23 jul. 2019. Disponível em: https://www.gazetadopovo.com.br/parana/novos-peritos-policia-pr. Acesso em: 3 dez. 2021.

ANDRÉS, Moisés Barrio. **Ciberdelitos Amenazas criminales del ciberespacio**. Madrid: Reus, 2017.

ARBULU, Rafael. WhatsApp é o app mais usado por brasileiros. **Olhar Digital**, 21 dez. 2020. Disponível em: bit.ly/3vgFHU2. Acesso em: 29 nov. 2021.

ÁVILA, Thiago André Pierobom de. **Fundamentos do controle externo da atividade policial**. Belo Horizonte: D'Plácido, 2016.

AVOLIO, Luiz Francisco Torquato. **Provas Ilícitas**: interceptações telefônicas, ambientais e gravações clandestinas. 7. ed. São Paulo: Thomson Reuters Brasil, 2019.

BADARÓ, Gustavo Henrique. **Epistemologia judiciária e prova penal** [livro eletrônico]. São Paulo: Thomson Reuters Brasil, 2019.

BADARÓ, Gustavo Henrique. **Processo Penal**. 10. ed. São Paulo: Thomson Reuters Brasil, 2022.

BADARÓ, Gustavo. A cadeia de custódia e sua relevância para a prova penal. In: SIDI, Ricardo; LOPES, Anderson B. (Org.). **Temas atuais da investigação preliminar no processo penal**. Belo Horizonte: D'Plácido, 2018. p. 517-538.

BADARÓ, Gustavo. Os standards metodológicos de produção na prova digital e a importância da cadeia de custódia. **Boletim IBCCRIM**, São Paulo, v. 29, n. 343, jun. 2021. Disponível em: https://www.ibccrim.org.br/js/pdf-js/web/viewer.html?file=/media/publicacoes/arquivos_pdf/revista-31-05-2021-10-44-29-869137.pdf. Acesso em: 05 dez. 2022.

BANDEIRA DE MELLO, Celso Antônio. **Curso de Direito Administrativo**. 27. ed. São Paulo: Malheiros, 2010.

BARRETO, Alesandro Gonçalves; KUFA, Karina; SILVA, Marcelo Mesquita. **Cibercrimes e seus reflexos no direito brasileiro**. 2. ed. São Paulo: JusPodivm, 2021.

BARROS, Marco Antonio Loschiavo Leme de. **Tribunais, complexidade e decisão**: o argumento consequencialista no direito brasileiro. 2018. 95 f. Tese (Doutorado em Direito) – Universidade de São Paulo, São Paulo, 2018. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2139/tde-30102020-152804/publico/6476260_Tese_Parcial.pdf. Acesso em: 18 ago. 2021.

BARROS, Renata Furtado de. **Guerra cibernética**: os novos desafios do direito internacional. Belo Horizonte: D'Plácido. 2021.

BELOTTO, Ana M. de S.; MADRUGA, Antenor; TOSI, Mariana T. Dupla incriminação na cooperação jurídica internacional. **Boletim IBCCRIM**, São Paulo, v. 20, n. 237, p. 15-16, ago. 2012.

BETTINE, Marco. **A teoria do agir comunicativo de Jüger Habermas**: bases conceituais. São Paulo: EACH, 2021. E-book.

BEUTH, Patrick. Bundestag genehmigt Staatstrojaner für alle. Die Bundespolizei sowie alle 19 Nachrichtendienste in Deutschland dürfen künftig Computer und Smartphones von Verdächtigen hacken. Die wichtigsten Bestandteile der neuen Regelungen – und erste Reaktionen. **Spiegel Netzwelt**, 10 Juni 2021. Disponível em: https://www.spiegel.de/netzwelt/netzpolitik/bundestag-genehmigt-staatstrojaner-fuer-alle-a-d01006d4-a530-41c9-ad69-21a3990acfa8. Acesso em: 17 jun. 2021.

BITENCOURT, Cezar Roberto. **Código Penal Comentado**. 8. ed. São Paulo: Saraiva, 2014.

BLANCO, Kenneth. An important Court opinion holds lawful warrants can be used to obtain evidence from U.S. internet service providers when those providers store evidence outside the U.S. **U. S. Department of Justice**, Washington, DC, 6 Feb. 2017. Disponível em: https://www.justice.gov/archives/opa/blog/important-court-opinion-holds-lawful-warrants-can-be-used-obtain-evidence-us-internet. Acesso em: 20 set. 2022.

BOLAMPERTI, Anne; FOWLER, Patrick X. What Does the New Utah Electronic Data Privacy Law Do? **JD Supra**, May 2019. Disponível em: https://www.jdsupra.com/legalnews/what-does-the-new-utah-electronic-data-72688. Acesso em: 19 nov. 2021.

BORGES, Ademar. O direito estrangeiro no aperfeiçoamento da jurisdição constitucional brasileira. **Jota**, 16 nov. 2021. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/penal-em-foco/direito-estrangeiro-jurisdicao-constitucional-brasileira-16112021. Acesso em: 19 nov. 2021.

BRANCO, Dácio Castelo. Criptografia pós-quântica? EUA investem em segurança de dados mais eficaz. **Canaltech**, 4 nov. 2021. Disponível em: https://canaltech.com.br/seguranca/criptografia-pos-quantica-eua-investem-em-seguranca-de-dados-mais-eficaz-200842. Acesso em: 02 nov. 2021.

BRANDÃO, Hemerson. Empresa alerta sobre grave falha de segurança no WhatsApp Web. **Minha Operadora**, jul. 2021. Disponível em: https://www.minhaoperadora.com.br/2021/07/empresa-alerta-sobre-grave-falha-de-seguranca-no-whatsapp-web.html. Acesso em: 30 nov. 2021.

BRASIL. Câmara dos Deputados. Anteprojeto de Lei. Altera os arts. 157, 563, 564, 567 e 571 a 573 e acrescenta o art. 570-A ao do Decreto-Lei n. 3.689, de 3 de outubro de 1941 - Código de Processo Penal, para redefinir o conceito de provas ilícitas e revisar as hipóteses de nulidade. **Diário Oficial da União**, Brasília, DF, 10 dez. 2015. Disponível em: https://dezmedidas.mpf.mp.br/apresentacao/conheca-as-medidas/docs/medida_7_versao-2015-06-25.pdf. Acesso em: 02 nov. 2022.

BRASIL. Câmara dos Deputados. **Árvore de Apensados - PL 5285/2009**. Disponível em:

https://www.camara.leg.br/proposicoesWeb/prop_arvore_tramitacoes?idProposicao=436096. Acesso em: 26 out. 2022.

BRASIL. Câmara dos Deputados. MSC 412/2020 Inteiro teor. Texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001, com fins de adesão brasileira ao instrumento. **Câmara dos Deputados**, Brasília, DF, 23 jul. 2020. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2258985. Acesso em: 12 dez. 2021.

BRASIL. Câmara dos Deputados. **MSC 412/2020**. Texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001, com fins de adesão brasileira ao instrumento. Brasília, DF, 30 jul. 2020. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2258985. Acesso em: 18 nov. 2021.

BRASIL. Câmara dos Deputados. Projeto de Lei 2630/2020. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1909983&filename=PL+2630/2020. Acesso em: 25 nov. 2022.

BRASIL. Câmara dos Deputados. Projeto de Lei n. 4.939/2020. Autor: Hugo Leal. **Câmara dos Deputados**, Brasília, DF, 15 out. 2020. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1936366&filename=PL+4939/2020. Acesso em: 6 jul. 2022.

BRASIL. Câmara dos Deputados. Projeto de Lei n. 5285/2009. Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=659491&filename=PL+5285/2009. Acesso em: 26 out. 2022.

BRASIL. Câmara dos Deputados. Projeto de Lei n. 8045/2010. Código de Processo Penal. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1638152&filename=PL+8045/2010. Acesso em: 03 nov. 2022.

BRASIL. Câmara dos Deputados. Projeto de Lei n. 9.808/2018. Acrescenta os parágrafos 5° e 6º ao art. 10 da Lei n. 12.965, de 23 de abril de 2014, para dispor sobre o acesso a dados de comunicação por meio de aplicativos de internet para fins de persecução criminal, nos casos que especifica. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1649924. Acesso em: 28 out. 2022.

BRASIL. Conselho da Justiça Federal. **Jurisprudência Unificada**. Disponível em: https://www2.cjf.jus.br/jurisprudencia/unificada. Acesso em: 21 dez. 2022.

BRASIL. Constituição da República Federativa do Brasil de 1988. **Diário Oficial da União**, Brasília, DF, 5 out. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 8 jul. 2022.

BRASIL. Decreto n. 678, de 6 de novembro de 1992. Promulga a Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), de 22 de novembro de 1969. **Diário Oficial da União**, Brasília, DF, 9 nov. 1992. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/d0678.htm. Acesso em 12 set. 2022.

BRASIL. Decreto n. 5.015, de 12 de março de 2004. Promulga a Convenção das Nações Unidas contra o Crime Organizado Transnacional. **Diário Oficial da União**, Brasília, DF, 15 mar. 2004. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/decreto/d5015.htm. Acesso em 19 set. 2022.

BRASIL. Emenda Constitucional n. 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. **Diário Oficial da União**, Brasília, DF, 11 fev. 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm. Acesso em: 26 out. 2022.

BRASIL. Lei n. 9605, de 12 de fevereiro de 1998. Dispõe sobre as sanções penais e administrativas derivadas de condutas e atividades lesivas ao meio ambiente, e dá outras providências. **Diário Oficial da União**, Brasília, DF, 13 fev. 1998. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9605.htm. Acesso em: 27 out. 2022.

BRASIL. Lei n. 11.343, de 23 de agosto de 2006. Institui o Sistema Nacional de Políticas Públicas sobre Drogas - Sisnad; prescreve medidas para prevenção do uso indevido, atenção e reinserção social de usuários e dependentes de drogas; estabelece normas para repressão à produção não autorizada e ao tráfico ilícito de drogas; define crimes e dá outras providências. **Diário Oficial da União,** Brasília, DF, 24 ago. 2006. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11343.htm. Acesso em 28 out. 2022.

BRASIL. Lei n. 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União,** Brasília, DF, 24 ABR. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 11 nov. 2022.

BRASIL. Lei n. 13.869, de 5 de setembro de 2019. Dispõe sobre os crimes de abuso de autoridade; [...]. **Diário Oficial da União,** Brasília, DF, 5 set. 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13869.htm. Acesso em: 26 out. 2022.

BRASIL. Lei n. 9.296, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. **Diário Oficial da União**, Brasília, DF, 25 jul. 1996, p. 13757. http://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 15 nov. 2021.

BRASIL. Ministério da Cidadania. **Classificação dos Dados**. Brasília, 30 abr. 2021. Disponível em: https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd/classificacao-dos-dados. Acesso em: 05 nov. 2022.

BRASIL. Ministério Público Federal. **Caso Lava Jato**. Disponível em: https://www.mpf.mp.br/grandes-casos/lava-jato/entenda-o-caso. Acesso em: 04 nov. 2022.

BRASIL. Ministério Público Federal. **MPF aponta vícios e pede anulação de decisão que determinou cautelares contra empresários por conversas em grupo de WhatsApp**. 9 set. 2022. Disponível em: https://www.mpf.mp.br/pgr/noticias-pgr/mpf-aponta-vicios-e-pede-anulacao-de-decisao-que-determinou-cautelares-contra-empresarios-por-conversas-em-grupo-de-whatsapp. Acesso em 15 nov. 2022.

BRASIL. Senado Federal. Projeto de Lei n. 236, de 2012. **Diário do Senado Federal**, Brasília, DF, 10 jul. 2012. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=3515262&ts=1613697834640&disposition=inline. Acesso em: 13 jun. 2021.

BRASIL. Superior Tribunal de Justiça. Interceptação Telefônica – I. **Jurisprudência em Teses**, Brasília, n. 117, 25 jan. 2019. Disponível em: https://scon.stj.jus.br/SCON/jt/toc.jsp. Acesso em: 9 jul. 2022.

BRASIL. Superior Tribunal de Justiça. **Quebra da cadeia de custódia não gera nulidade obrigatória da prova, define Sexta Turma**. Brasília, 9 dez. 2021. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/09122021-Quebra-da-cadeia-de-custodia-nao-gera-nulidade-obrigatoria-da-prova--define-Sexta-Turma.aspx. Acesso em: 12 dez. 2021.

BRASIL. Superior Tribunal de Justiça. RHC 133430/PE. AgRg no RHC 133430/PE. Relator: Min. Nefi Cordeiro. **Diário de Justiça Eletrônico**, Brasília, DF, 26 fev. 2021.

BRASIL. Superior Tribunal de Justiça. RHC 99.735. Relatora: Min. Laurita Vaz. **Diário de Justiça Eletrônico**, Brasília, DF, 12 dez. 2018.

BRASIL. Superior Tribunal de Justiça. RHC 99.735/SC. Relatora: Min. Laurita Vaz. **Diário de Justiça Eletrônico**, Brasília, DF, 12 dez. 2018. Disponível em: https://scon.stj.jus.br/SCON/jurisprudencia/toc.jsp?i=1&b=ACOR&livre=((%27RHC%27.clap.+e+@num=%2799735%27)+ou+(%27RHC%27+adj+%2799735%27.suce.))&thesaurus=JURIDICO&fr=veja. Acesso em: 07 dez. 2021.

BRASIL. Supremo Tribunal Federal. **ADC 51**. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5320379. Acesso em: 24 nov. 2022.

BRASIL. Supremo Tribunal Federal. **ADI 5.527/DF**. Relatora: Min. Rosa Weber. Disponível em:

http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI5527voto.pdf. Acesso em: 21 jun. 2021.

BRASIL. Supremo Tribunal Federal. **ADPF 403/SE**. Min. Edson Fachin. Disponível em: http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADPF403voto.pdf. Acesso em: 21 jun. 2021.

BRASIL. Supremo Tribunal Federal. AgRg no RHC 133430/PE. Relator: Min. Nefi Cordeiro. **Diário de Justiça Eletrônico**, Brasília, DF, 26 fev. 2021.

BRASIL. Supremo Tribunal Federal. **Audiência pública - Bloqueio judicial do WhatsApp e Marco Civil da Internet (1/4)**. 2017. Disponível em: https://www.youtube.com/watch?v=3TNsQCNIOO0. Acesso em: 06 nov. 2022.

BRASIL. Supremo Tribunal Federal. Extradição n. 669. Relator: Min. Celso de Mello. Julgamento em 6 de março de 1996. **Diário da Justiça**, 29 mar. 1996.

BRASIL. Supremo Tribunal Federal. **Gilmar Mendes vota pela possibilidade de solicitação de dados diretamente a provedores no exterior**. 2022. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=495011&ori=1. Acesso em: 24 nov. 2022.

BRASIL. Supremo Tribunal Federal. Habeas Corpus n. 132.062/RS, 1ª Turma. Relator: Min. Marco Aurélio; Relator do Acórdão: Ministro Edson Fachin. Brasília, 22 nov. 2016.

BRASIL. Supremo Tribunal Federal. Habeas Corpus n. 132.115/PR. Relator: Ministro Dias Toffoli. Brasília, 06 abr. 2018.

BRASIL. Supremo Tribunal Federal. Habeas Corpus n. 168.052/SP, 2ª Turma. Relator: Min. Gilmar Mendes, Brasília, 02 dez. 2020.

BRASIL. Supremo Tribunal Federal. Medida Cautelar em ADI n. 7.261/DF. Relator: Min. Edson Fachin. Brasília, DF, 22 out. 2022. Disponível em: https://www.conjur.com.br/dl/adi7261-indeferid.pdf. Acesso em: 25 nov. 2022.

BRASIL. Supremo Tribunal Federal. **Pedido de vista adia julgamento sobre obtenção de dados de provedores de internet no exterior**. Out. 2022. Disponível em: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=495363&ori=1. Acesso em: 24 nov. 2022.

BRASIL. Supremo Tribunal Federal. Tema 1.148 – Limites para decretação judicial da quebra de sigilo de dados telemáticos, no âmbito de procedimentos penais, em relação a pessoas indeterminadas. Relatora: Min. Rosa Weber. Disponível em: http://www.stf.jus.br/portal/jurisprudenciaRepercussao/detalharProcesso.asp?numeroTema=1148. Acesso em: 2 dez. 2021.

BRASIL. Supremo Tribunal Federal. Tema 661 – STF: Possibilidade de prorrogações sucessivas do prazo de autorização judicial para interceptação telefônica. **Diário da Justiça Eletrônico**, 6 jun. 2022.

BRASIL. Supremo Tribunal Federal. Tema 977 – Aferição da licitude da prova produzida durante o inquérito policial relativa ao acesso, sem autorização judicial, a registros e informações contidos em aparelho de telefone celular, relacionados à conduta delitiva e hábeis a identificar o agente do crime. Relator: Min. Dias Toffoli. Disponível em: http://www.stf.jus.br/portal/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=5173898&numeroProcesso=1042075&classeProcesso=ARE&numeroTema=977. Acesso em: 3 dez. 2021.

BRASIL. Tribunal Superior Eleitoral. **TSE e plataformas digitais discutem reforço contra desinformação no 2º turno**. Brasília, 19 out. 2022. Disponível em: https://www.tse.jus.br/comunicacao/noticias/2022/Outubro/tse-e-plataformas-digitais-discutem-reforco-contra-desinformacao-no-2o-turno-1. Acesso em: 25 nov. 2022.

BRODOWSKI, Dominik. **Cibercrimen y Protección de la Seguridad Informática**. Tradução: María Belén Linares. Buenos Aires: Ad-Hoc, 2021.

BUSATO, Paulo César. Delitos de posse e ação significativa – crítica aos Besitzdelikte a partir da Concepção Significativa da Ação. **Sequência**, Florianópolis, n. 73, p. 75-112, maio/ago. 2016.

BUSATO, Paulo César. **Direito penal**: parte especial. 2. ed. São Paulo: Atlas, 2016. v. 1.

BUSATO, Paulo César. **Direito penal**: parte geral. 6. ed. São Paulo: Tirant lo Blanch, 2022.

BUSATO, Paulo César. Razões criminológicas, político-criminais e dogmáticas para a adoção da responsabilidade penal de pessoas jurídicas na reforma do Código Penal brasileiro. In: BUSATO, Paulo César; GUARAGNI, Fábio André. **Responsabilidade penal da pessoa jurídica**: fundamentos criminológicos, superação de obstáculos dogmáticos e requisitos legais do interesse e benefício do ente coletivo para a responsabilização criminal. Curitiba: Juruá, 2012.

BUSATO, Paulo César. Razões político-criminais para a responsabilidade penal das pessoas jurídicas. In: BUSATO, Paulo César; GRECO, Luís (Coord.). **Responsabilidade penal de pessoas jurídicas**: seminário Brasil-Alemanha. Florianópolis: Tirant Lo Blanch, 2018. p. 11-68.

CAMPILONGO, Celso Fernandes. **O direito na sociedade complexa**. 2. ed. São Paulo: Saraiva, 2013.

CAMPOS, Ricardo. Lei alemã ou movimento global? O debate sobre regulação de redes contextualizado. **Consultor Jurídico**, 24 nov. 2020. Disponível em: https://www.conjur.com.br/2020-nov-24/direito-digital-lei-alema-ou-movimento-global-contextualizando-debate-regulacao-redes. Acesso em: 20 nov. 2021.

CAMPOS, Ricardo. **Metamorfoses do direito global**: sobre a interação entre Direito, tempo e tecnologia. São Paulo: Contracorrente, 2022.

CAMPOS, Ricardo; MARANHÃO, Juliano S. A. Os registros públicos e os fundamentos da proteção de dados. In: WOLKART, Erik Navarro et al. (Coord.). **Direito, processo e tecnologia**. 2. ed. São Paulo: Thomson Reuters, 2021.

CANALTECH. **Telegram**. Disponível em: https://canaltech.com.br/empresa/telegram. Acesso em: 29 nov. 2021.

CARUSO, Tiago. **Responsabilidade penal nas decisões embasadas em pareceres técnicos e jurídicos**. São Paulo: Marcial Pons, 2020.

CASELLI, Guilherme. **Manual de Investigação Criminal**. São Paulo: JusPodivm, 2021.

CAVALHEIRO, Lucilene. ISO 27037 Diretrizes para identificação, coleta, aquisição e preservação de evidência digital. **Academia de Forense Digital**, jan. 2019. Disponível em: https://academiadeforensedigital.com.br/iso-27037-identificacao-coleta-aquisicao-e-preservacao-de-evidencia. Acesso em: 07 dez. 2021.

CIS. **Crypto Policy Project**. Disponível em: https://cyberlaw.stanford.edu/our-work/projects/crypto-policy-project. Acesso em: 03 dez. 2021.

CONGRESS.GOV. **S.3538 - EARN IT Act of 2022**. 2022. Disponível em: https://www.congress.gov/bill/117th-congress/senate-bill/3538/text. Acesso em: 18 out. 2022.

CONSELHO DA EUROPA. **Convenção sobre o Cibercrime**. Budapeste, 23 nov. 2001. Disponível em: http://https://rm.coe.int/16802fa428. Acesso em: 19 dez. 2022.

CORTE IDH. Caso Escher e Outros vs. Brasil, de 6 de julho de 2009. Disponível em: www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf. Acesso em: 17 nov. 2022.

COSTA JÚNIOR, Ivan Jezler. **Prova penal digital**: tempo, risco e busca telemática. Florianópolis: Tirant Lo Blanch, 2019.

COSTA, Daniel Tempski Ferreira da. O pós-fundacionalismo como fundamento de uma nova técnica de decisão judicial em casos de repercussão globalizada: a força dos precedentes estrangeiros no julgamento interno em defesa de um pluralismo jurídico democrático. In: SOUZA NETTO, José Laurindo; GIACOIA, Alberto; CAMBI, Eduardo (Coord.). **Direito, gestão e democracia**: estudos em homenagem ao Ministro Felix Fischer. Curitiba: Clássica, 2022. p. 115-134.

COSTA, Daniel Tempski Ferreira da; ROSA, Luísa Walter da. A resolução de casos difíceis a partir do pensamento de Neil MacCormick: a necessidade da análise de precedentes das Supremas Cortes de nações democráticas. **Interfaces Científicas**:

Direito, Aracaju, v. 9, n. 1, p. 110-123, 2022. DOI: 10.17564/2316-381X.2022v9n1p110-123. Acesso em: 30 jun. 2022.

COSTA, Leandro S. Algumas considerações sobre a possibilidade de um enfoque antropológico na filosofia de Ludwig Wittgenstein. **Espaço Acadêmico**, Maringá, v. 15, n. 179, p. 52-60, abr. 2016.

CUERDA ARNAU, María Luisa. Limites constitucionales de la comisión por omisión. **Justiça e Sistema Criminal**, Curitiba, v. 6, n. 10, p. 97-119, jan./jun. 2014. Disponível em: https://revistajusticaesistemacriminal.fae.edu/direito/article/view/15/13. Acesso em: 4 jul. 2022.

CURRY, David. Messaging App Revenue and Usage Statistics (2022). **Business of Apps**, 13. Sep. 2022. Disponível em: https://www.businessofapps.com/data/messaging-app-market/#:~:text=WhatsApp%20is%20the%20most%20popular%20messaging%20app%20worldwide%2C%20and%20is,Middle%20East%20and%20South%20America. Acesso em: 07 nov. 2022.
DAMAŠKA, Mirjan R. **Evidence Law Adrift**. New Haven: Yale University, 1997.

DATASAFER. **35.057 Atendimentos e 4.441.595 Denúncias.** Disponível em: https://indicadores.safernet.org.br/indicadores.html. Acesso em 19 set. 2022.

DELGADO, Vladimir Chaves. **Cooperação Internacional em matéria penal na Convenção sobre o Cibercrime**. 2007. 315 f. Dissertação (Mestrado em Direito das Relações Internacionais) – Centro Universitário de Brasília, 2007. Disponível em: https://repositorio.uniceub.br/jspui/bitstream/123456789/3562/3/vladimir.pdf. Acesso em: 22 nov. 2022.

DELONG, John et al. **Don't Panic Making Progress on the "Going Dark" Debate**. Cambridge: Berkman, 2016. Disponível em: https://cyber.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf. Acesso em: 16 nov. 2021.

DEU, Teresa Armenta. **A prova ilícita**: um estudo comparado. Tradução: Nereu José Giacomolli. São Paulo: Marcial Pons, 2014.

DEUTSCHER BUNDESTAG. **Pro und Contra Staats-trojaner bei der Anhörung zur Strafrechts-reform**. Berlin, 2017. Disponível em: https://www.bundestag.de/dokumente/textarchiv/2017/kw22-pa-recht-strafrecht/508168. Acesso em: 10 set. 2021.

DEUTSCHLAND. Annual preview: Preview for 2022 (in German). **First Senate**. Disponível em: https://www.bundesverfassungsgericht.de/EN/Verfahren/Jahresvorausschau/vs_2022/vorausschau_2022.html. Acesso em: 21 out. 2022.

DEUTSCHLAND. Bundesministeriums des Innern. **Gesetz über die Bundespolizei**. Ausfertigungsdatum: 19.10.1994. Disponível em: https://www.gesetze-im-internet.de/bgsg_1994/BJNR297900994.html. Acesso em: 20 out. 2022.

DEUTSCHLAND. Bundesverfassungsgericht. Erfolglose **Verfassungsbeschwerde gegen hessische Vorschriften zum verdeckten Zugriff auf informationstechnische Systeme**. Pressemitteilung Nr. 20/2022 vom 9. März 2022. Disponível em: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2022/bvg22-020.html. Acesso em: 20 out. 2022.

DEUTSCHLAND. Bundesverfassungsgericht. Leitsätze zum Beschluss des Ersten Senats vom 8. Juni 2021. **BvR 2771/18**. Disponível em: bit.ly/3P7EQhz. Acesso em: 20 out. 2022.

DEUTSCHLAND. Deutscher Bundestag. **Grundgesetz für die Bundesrepublik Deutschland**. Disponível em: bit.ly/3Yeg6IT. Acesso em: 13 set. 2022.

DEUTSCHLAND. Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens. **Bundesgesetzblatt Teil I**, Bonn, n. 58, Aug. 2017. Disponível em: https://www.bgbl.de/xaver/bgbl/start.xav?start=%2F%2F*%5B%40attr_id%3D%27I_2017_58_inhaltsverz%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s3202.pdf%27%5D__1529934677611. Acesso em: 9 set. 2021.

DIAS, Eduardo R.; ROCHA, Robert F. A Constituição líquida: mutação constitucional e expansão de direitos fundamentais na hipermodernidade. **Revista de Direitos Fundamentais & Democracia**, Curitiba, v. 24, n. 1, p. 143-160, jan./abr. 2019. DOI: 10.25192/issn.1982-0496.rdfd.v24i11423. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/1423/573. Acesso em: 02 nov. 2021.

DISSENHA, Rui Carlo. Cooperação jurisdicional penal internacional: o difícil conflito entre os planos jurídico e político na justiça penal. In: SOUZA, André Peixoto de (Org.). **Estado, poder e jurisdição**. Rio de Janeiro: GZ, 2015. p. 121-144.

DONEDA, Danilo; MACHADO, Diego (Org.). **A criptografia no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2020, RB-3.1. E-book.

DUTRA, Deo Campos. Método(s) em direito comparado. **Revista da Faculdade de Direito – UFPR**, Curitiba, v. 61, n. 3, p. 189-212, set./dez. 2016. Disponível em: https://revistas.ufpr.br/direito/article/view/46620. Acesso em: 10 ago. 2021.

EBERHARDT, Marcos; PIPPI, Marcos. Prova criminal: WhatsApp e cadeia de custódia. **Consultor Jurídico**, 13 out. 2021. Disponível em: https://www.conjur.com.br/2021-out-13/eberhardt-pippi-prova-criminal-whatsapp-cadeia-custodia?s=08. Acesso em: 07 dez. 2021.

EBERHARDT, Marcos; PIPPI, Marcos. Prova criminal: WhatsApp e cadeia de custódia. **Consultor Jurídico**, 13 out. 2021. Disponível em:

https://www.conjur.com.br/2021-out-13/eberhardt-pippi-prova-criminal-whatsapp-cadeia-custodia?s=08. Acesso em: 07 dez. 2021.

ELECTRONIC FRONTIER FOUNDATION. **Section 230 of the Communications Decency Act**. Disponível em: https://www.eff.org/issues/cda230#:~:text=Section%20230%20says%20that%20%22No,%C2%A7%20230. Acesso em: 19 set. 2022.

ENCRYPTION BACKDOOR. **Techopedia**, fev. 2020. Disponível em: https://www.techopedia.com/definition/3743/encryption-backdoor. Acesso em: 30 out. 2021.

ESCOLA SUPERIOR DO MINISTÉRIO PÚBLICO DA UNIÃO (ESMPU). **Especialistas discutem anteprojeto da LGPD Penal**. Brasília, 15 jan. 2021. Disponível em: https://escola.mpu.mp.br/a-escola/comunicacao/noticias/especialistas-discutem-anteprojeto-da-lgpd-penal. Acesso em: 24 nov. 2022.

ESPAÑA. Ley 34/2002. **Boletín Oficial del Estado**, n. 166, 12 jul. 2002. Disponível em: https://www.boe.es/eli/es/l/2002/07/11/34/con. Acesso em: 21 out. 2022.

FAIRBANKS, R. Masterpiece or Mess: The Mosaic Theory of the Fourth Amendment Post-Carpenter. **Berkeley Journal of Criminal Law**, v. 26, n. 1, p. 71-119, 2021. Disponível em: https://doi.org/10.15779/Z38DZ03287. Acesso em: 14 nov. 2021.

FERREIRA, Marco Aurélio Gonçalves. A interceptação telefônica em perspectiva comparada. In: SANTORO, Antonio Eduardo Ramires; MADURO, Flávio Mirza (Org.). **A interceptação telefônica em perspectiva comparada**. Belo Horizonte: D'Plácido, 2017. p. 271-289.

FISHER, Alexis. First Amendment Issues with the Amazon Alexa. **Ristenpart Law**. Disponível em: https://www.ristenpartlaw.com/news-and-updates/first-amendment-issues-with-the-amazon-alexa. Acesso em: 5 jun. 2021.

FLADE, Florian; TANRIVERDI, Hakan. BKA kann bei WhatsApp mitlesen. **Tagesschau**, 21 Juli 2020. Disponível em: https://www.tagesschau.de/investigativ/wdr/bka-whatsapp-101.html. Acesso em: 10 maio 2021.

FONTENLA, Carolina Paulino. Desafios da cooperação entre empresas de internet e Poder Público. **Migalhas**, 9 jun. 2021. Disponível em: https://www.migalhas.com.br/depeso/346738/desafios-da-cooperacao-entre-empresas-de-internet-e-poder-publico. Acesso em: 22 jun. 2021.

FREITAS JÚNIOR, Adair Dias de; JORGE, Higos Vinícius Nogueira; GARZELLA, Oleno Carlos Faria. **Manual de interceptação telefônica e telemática**. 2. ed. São Paulo: JusPodivm, 2021.

FRIEDMAN, Richard D. Anchors and Flotsam: Is Evidence Law 'Adrift'? Review of Evidence Law Adrift, by M. R. Damaška. **Yale Law Journal**, v. 107, n. 6, p. 1921-

1967, 1998. Disponível em: https://repository.law.umich.edu/reviews/14. Acesso em: 05 nov. 2021.

FUNDAÇÃO GETÚLIO VARGAS (FGV). **CryptoMap**: uma pesquisa sobre o debate jurídico da criptografia. Disponível em: https://www.fgv.br/direitosp/cryptomap/#home. Acesso em: 29 nov. 2021.

FURLANETO NETO, Mário; SANTOS, José E. L. dos. Apontamentos sobre a cadeia de custódia da prova digital no Brasil. **Em Tempo**, Marília, v. 20, n. 1, nov. 2020. Disponível em: https://revista.univem.edu.br/emtempo/article/view/3130. Acesso em: 26 jun. 2021.

GALÁN MUÑOZ, Alfonso. A responsabilidade penal dos provedores de serviço na internet pela divulgação de conteúdos ilícitos: uma reflexão inicial sobre o regime espanhol e o brasileiro. **Justiça e Sistema Criminal**, Curitiba, v. 6, n. 11, p. 73-100, jul./dez. 2014. Disponível em: https://revistajusticaesistemacriminal.fae.edu/direito/article/view/30. Acesso em: 3 jul. 2022.

GARCIA, Rafael de Deus. Pode a autoridade policial acessar os dados do celular do indivíduo sem autorização judicial? **Empório do Direito.com.br**, Florianópolis, jan. 2018. Disponível em: http://emporiododireito.com.br/leitura/pode-a-autoridade-policial-acessar-os-dados-do-celular-do-individuo-sem-autorizacao-judicial. Acesso em: 09 set. 2020.

GHEDIN, Rodrigo. Google é multado por não interceptar e-mails durante a Operação Lava Jato da Polícia. **Gizmodo**, 16 dez. 2014. Disponível em: https://gizmodo.uol.com.br/google-emails-lava-jato/. Acesso em: 29 nov. 2022.

GIACOMOLLI, Nereu José. **O devido Processo Penal**: abordagem conforme a Constituição Federal e o Pacto de São José da Costa Rica. São Paulo: Atlas, 2014.

GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. **O direito de proteção de dados no processo penal e na segurança pública**. Rio de Janeiro: Marcial Pons, 2021.

GLOBAL INTERNET FORUM TO COUNTER TERRORISM (GIFCT). Disponível em: https://gifct.org/. Acesso em: 01 nov. 2022.

GLOECKNER, Ricardo Jacobsen. **Nulidades no Processo Penal**. 3. ed. São Paulo: Saraiva, 2017.

GLOECKNER, Ricardo Jacobsen; EILBERG, Daniela Dora. Busca e apreensão de dados em telefones celulares: novos desafios diante dos avanços tecnológicos. **Revista Brasileira de Ciências Criminais**, São Paulo, v. 156, p. 353-393, jun. 2019.

GOGONI, Ronaldo. Como funciona a criptografia de ponta a ponta do WhatsApp. **Tecnoblog**, 2019. Disponível em: https://tecnoblog.net/299425/como-funciona-a-criptografia-de-ponta-a-ponta-do-whatsapp. Acesso em: 29 nov. 2021.

GOMES FILHO, Antônio Magalhães. Notas sobre a terminologia da prova (reflexos no processo penal brasileiro). In: YARSHELL, Flávio Luiz; MORAES, Maurício Zanoide de (Org.). **Estudos em homenagem à Professora Ada Pellegrini Grinover**. São Paulo: DPJ, 2005. p. 303-318.

GOMES, Helton Simões. WhatsApp: "PL para rastrear mensagem classifica todos como suspeitos". **UOL**, São Paulo, 23 jul. 2020. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/06/23/rastrear-mensagem-e-por-tornozeleira-eletronica-em-usuario-diz-whatsapp.htm. Acesso em: 08 ago. 2021.

GONZÁLEZ CUSSAC, José Luis; BUSATO, Paulo César; CABRAL, Rodrigo Leite Ferreira. **Compêndio de direito penal brasileiro**: parte geral. Valencia: Tirant lo Blanch, 2017.

GRECO, Luís; GLEIZER, Orlandino. A infiltração online no processo penal: notícia sobre a experiência alemã. **Revista Brasileira de Direito Processual Penal**, Porto Alegre, v. 5, n. 3, p. 1483-1518, set./dez. 2019. Disponível em: http://www.ibraspp.com.br/revista/index.php/RBDPP/article/view/278. Acesso em: 20 nov. 2021.

GUIDI, Guilherme Berti de Campos. O Cloud Act e os reflexos na sistemática de produção de provas no estrangeiro. **Revista de Direito e as Novas Tecnologias**, São Paulo, v. 3, abr./jun. 2019. 3. Disponível em: https://bd.tjdft.jus.br/jspui/handle/tjdft/49610. Acesso em: 24 nov. 2022.

HARVARD UNIVERSITY. **Don't Panic**: Making Progress on the "Going Dark" Debate. Cambridge, 2016. Disponível em: https://dash.harvard.edu/handle/1/28552576. Acesso em: 16 nov. 2021.

HASSEMER, Winfried. **Introdução aos Fundamentos do Direito Penal**. Tradução: Pablo Rodrigo Alflen da Silva. Porto Alegre: S. A. Fabris, 2005.

HAUFE ONLINE REDAKTION. Verfassungsklage gegen neue Abhörmöglichkeiten der Geheimdienste durch Quellen-TKÜ. **Haufe**, 5 July 2021. Disponível em: https://www.haufe.de/compliance/recht-politik/verfassungsklage-gegen-online-durchsuchung-mit-staatstrojaner_230132_463812.html. Acesso em: 06 dez. 2021.

HAYES, Julian. Online safety: the encryption dilemma - trade-offs. **United Kingdom**, August 18 2022. Disponível em: https://www.lexology.com/library/detail.aspx?g=532d98ba-6539-4d6a-a33b-f2a838b7117c. Acesso em 14 out. 2022.

HESPANHA, Antônio Manuel. **Pluralismo jurídico e direito democrático**. São Paulo: Annablume, 2013.

HESSE, Konrad. **A força normativa da Constituição**. Tradução: Gilmar Mendes. Porto Alegre: S. A. Fabris, 1991.

HÖFFE, Otfried. **Derecho intercultural**. Tradução: Rafael Sevilla. Barcelona: Gedisa, 2008.

HOFFMANN-RIEM, Wolfgang. A Proteção Jurídica Fundamental da Confidencialidade e da Integridade dos Sistemas Técnicos de Informação de Uso Próprio. Tradução: Italo R. Fuhrmann. **Direito Público**, Brasília, v. 18, n. 100, p. 457-499, out./dez. 2021. DOI: https://doi.org/10.11117/rdp.v18i100.6212. Acesso em: 21 dez. 2022.

HUERTA, Pablo Pascual. **La génesis del derecho fundamental a la protección de datos personales**. 2017. 369 f. Tesis (Doctorado en Derecho Constitucional) – Universidad Complutense de Madrid, Madrid, 2017. Disponível em: https://eprints.ucm.es/id/eprint/43050/1/T38862.pdf. Acesso em: 10 nov. 2021.

ITALIA. **Codice di Procedura Penale**. Disponível em: https://www.polpenuil.it/attachments/048_codice_di_procedura_penale.pdf. Acesso em: 04 dez. 2022.

JARRETT, H. Marshall; BAILIE, Michael W. **Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations**. 3. ed. Washington, DC: Office of Legal Education - Executive Office for United States Attorneys, 2009. Disponível em: https://www.justice.gov/file/442111/download. Acesso em: 19 set. 2022.

JULIO, Clara. Malware backdoor: entenda esse tipo de ameaça e saiba como evitar. **Backup Garantido**, 19 jan. 2021. Disponível em: https://backupgarantido.com.br/blog/malware-backdoor. Acesso em: 03 dez. 2021.

KERR, Orin S. The Case for the Third-Party Doctrine. **Michigan Law Review**, v. 107, n. 561, Feb. 2009. Disponível em: https://web.archive.org/web/20091007084048/http://www.michiganlawreview.org/assets/pdfs/107/4/kerr.pdf. Acesso em: 28 set. 2021.

KERR, Orin S. The Mosaic Theory of the Fourth Amendment. **Michigan Law Review**, v. 111, n. 3, p. 311, 2012.

KONNO JÚNIOR, Janio. Interceptação Telemática ou Busca e Apreensao de Dados em Nuvem e a Preservação da Cadeia de Custódia. In: JORGE, Higor Vinicius Nogueira (Coord.). **Tratado de Investigação Criminal Tecnológica**. 2. ed. Salvador: JusPodivm. 2021. p. 273-287.

KOZICKI, Katya; PUGLIESE, William Soares. Uma era de common law para o Brasil? In: Congresso Internacional de Direito Constitucional e Filosofa Política (2.: 2015: Belo Horizonte, MG). In: BUSTAMANTE, Thomas et al. (Org.). **Precedentes judicias, judicialização da política e ativismo judicial**. Belo Horizonte: Initia Via, 2016.

KUGLER, Mattew B.; STRAHILEVITZ, Lior. Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory. **The Supreme Court Review**, Chicago, n. 4, Oct. 2015. Disponível em:

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2629373. Acesso em: 08 jul. 2021.

LEAL, Mônia Clarissa Hennig; MORAES, Maria Valentina de. **Margem de apreciação nacional e diálogo institucional e entre cortes na perspectiva do Supremo Tribunal Federal e da Corte Interamericana de Direitos Humanos**. São Paulo: Tirant lo Blanch, 2021.

LEGAL INFORMATION INSTITUTE (LII). **18 U.S. Code Chapter 121 – Stored Wire And Electronic Communications and Transactional Records Access**. Disponível em: https://www.law.cornell.edu/uscode/text/18/part-I/chapter-121. Acesso em: 02 nov. 2021.

LEGAL INFORMATION INSTITUTE (LII). **47 U.S. Code § 230**: Protection for private blocking and screening of offensive material. Disponível em: https://www.law.cornell.edu/uscode/text/47/230. Acesso em: 18 out. 2022.

LEGRAND, Pierre. A Impossibilidade de "Transplantes Jurídicos". Tradução: Gustavo Castagna Machado. **Cadernos do Programa de Pós-Graduação em Direito/UFRGS**, Porto Alegre, v. 9, n. 1, p. 11-39, 2014. Disponível em: https://seer.ufrgs.br/ppgdir/article/view/49746/35160. Acesso em: 08 dez. 2021.

LEMOS, Bruno Espiñeira; QUINTIERI, Victor Minervino. **Técnicas especiais de investigação no processo penal**. Belo Horizonte: D'Plácido, 2017.

LEONARDI, Marcel. **Fundamentos de direito digital**. São Paulo: Thomson Reuters Brasil, 2019.

LEWIS, James A.; ZHENG, Denis E.; CARTER, William A. The Effect of Encryption on Lawful Access to Communication and Data. **CSIS**, 8 Feb. 2017. Disponível em: https://www.csis.org/analysis/effect-encryption-lawful-access-communications-and-data. Acesso em: 17 maio 2020.

LIGUORI, Carlos. Exploring Lawful Hacking as a Possible Answer to the "Going Dark" Debate. **Michigan Technology Law Review**, v. 26, n. 317, p. 317-347, 2020. Disponível em: https://repository.law.umich.edu/mtlr/vol26/iss2/5. Acesso em: 30 nov. 2021.

LIMA, Renato Brasileiro de. **Manual de processo penal**. 11. ed. São Paulo: JusPodivm, 2022, p. 610.

LOMAS, Natasha. Tech CEOs to face faster criminal liability under UK online safety law. **TechCrunch**, 16 mar. 2022. Disponível em: https://techcrunch.com/2022/03/16/online-safety-bill-parliament/. Acesso em 17 out. 2022.

LOMAS, Natasha. UK publishes draft Online Safety Bill. **Techcrunch**, 12 May 2021. Disponível em: https://techcrunch.com/2021/05/12/uk-publishes-draft-online-safety-bill. Acesso em: Acesso em: 06 dez. 2021.

LOPES, Anderson B. **Os conhecimentos fortuitos de prova no processo penal**. Belo Horizonte: D'Plácido, 2016.

LÓSSIO, Claudio Joel Brito. **Manual descomplicado de direito digital**: guia para profissionais do direito e da tecnologia. 2 ed. São Paulo: JusPodivm, 2021.

LOUBAK, Ana Letícia. WhatsApp agora tem opção para criptografar backup de conversas; entenda. **Techtudo**, 10 out. 2021. Disponível: https://www.techtudo.com.br/noticias/2021/10/whatsapp-agora-tem-opcao-para-criptografar-backup-de-conversas-entenda.ghtml. Acesso em: 30 nov. 2021.

MACASKILL, Ewen. 'Extreme surveillance' becomes UK law with barely a whimper. **The Guardian**, 19 Nov. 2016. Disponível em: https://www.theguardian.com/world/2016/nov/19/extreme-surveillance-becomes-uk-law-with-barely-a-whimper. Acesso em: Acesso em: 06 dez. 2021.

MACCORMICK, Neil. **Argumentação jurídica e teoria do direito**. São Paulo: Martins Fontes, 2006.

MACDONALD, C. Gov. Herbert signs bill requiring police obtain search warrants to access electronic information. **KSL.com**, Mar. 2019. Disponível em: https://www.ksl.com/article/46520524/gov-herbert-signs-bill-requiring-police-obtain-search-warrants-to-access-electronic-information. Acesso em: 15 nov. 2021.

MACHADO, Leonardo Marcondes. **Introdução crítica à investigação preliminar**. Belo Horizonte: D'Plácido, 2020.

MACHADO, Vitor Paczek; JEZLER JUNIOR, Ivan. A prova eletrônica-digital e a cadeia de custódia das provas: uma (re)leitura da Súmula Vinculante 14. **Boletim IBCCRIM**, São Paulo, v. 24, n. 288, nov. 2016.

MAGRO, Américo Ribeiro; ANDRADE, Landolfo. **Manual de direito digital**. São Paulo: Juspodivm, 2021.

MALAN, Diogo. Interceptação de comunicações telefônicas: standards dos sistemas interamericano e europeu de direitos humanos, p. 149-174. In: SANTORO, Antonio E. R.; MADURO, Flávio Mirza (Org.). **Interceptação telefônica**: 20 anos da Lei 9.296/96. Belo Horizonte: D'Plácido, 2016. p. 149-174.

MALWAREBYTES. **Tudo sobre hacking**. Disponível em: https://br.malwarebytes.com/hacker. Acesso em: 03 dez. 2021.

MANCUSO, Ronnie. A criptografia do WhatsApp foi furada? Fato ou mito? **Olhar Digital**, 9 set. 2021. Disponível em: https://olhardigital.com.br/2021/09/09/seguranca/a-criptografia-do-whatsapp-foi-furada-fato-ou-mito. Acesso em: 28 out. 2021.

MENDES, Carlos Hélder C. Furtado. **Tecnoinvestigação criminal**: entre a proteção de dados e a infiltração por software. Salvador: Juspodivm, 2020.

MENDES, Gilmar Ferreira; VALE, André Rufino do. A influência do pensamento de Peter Häberle no STF. **Conjur**, abr. 2009, p. 7. Disponível em: https://www.conjur.com.br/2009-abr-10/pensamento-peter-haberle-jurisprudencia-supremo-tribunal-federal?pagina=7. Acesso em: 18 nov. 2021.

MENDONÇA, Andrey Borges de. **Cooperação Internacional no Processo Penal**: a transferência de processos. São Paulo: Thomson Reuters, 2021.

MENDOZA, Melanie Claire F.; BRANDÃO, Luiz Mathias R. Do direito à privacidade à proteção de dados: das teorias de suporte e a exigência da contextualização. **Revista de Direito, Governança e Novas Tecnologias**, Brasília, v. 1, n. 2, p. 223-240, jan./jun. 2016. Disponível em: https://www.indexlaw.org/index.php/revistadgnt/article/view/830. Acesso em: 10 out. 2021.

MENEZES, Cyntia S. de; AGUSTINA, José R. Big data, inteligencia artificial y policía predictiva: bases para una adecuada regulación legal que respete los derechos fundamentales. In: KIEFER, Mariana (Coord.). **Cibercrimen III**. Buenos Aires: BdeF, 2020.

META. Disponível em: https://about.facebook.com/br/company-info. Acesso em: 29 nov. 2021.

MEYER, Jonathan E.; CARLSON, Sonja S. Supreme Court Reenters Fray on Privacy: Carpenter v. United States. **National Law Review**, June 2017. Disponível em: https://www.natlawreview.com/article/supreme-court-reenters-fray-privacy-carpenter-v-united-states. Acesso em: 02 nov. 2021.

MEYER, Jonathan E.; CARLSON, Sonja S. Supreme Court Reenters Fray on Privacy: Carpenter v. United States. **National Law Review**, June 2017. Disponível em: https://www.natlawreview.com/article/supreme-court-reenters-fray-privacy-carpenter-v-united-states. Acesso em: 02 nov. 2021.

MORAIS, Fausto Santos de. **Ponderação e arbitrariedade**: a inadequada recepção de Alexy pelo STF. Salvador: Juspodivm, 2010.

MOTOMURA, Marina. Quantos idiomas existem no mundo? **Superinteressante**, 25 maio 2011. Disponível em: https://super.abril.com.br/mundo-estranho/quantos-idiomas-existem-no-mundo. Acesso em: 6 jul. 2022.

MOURA, Grégore Moreira de. **Curso de direito penal informático**. Belo Horizonte: D'Plácido, 2021.

MULLIN, Joe. The FBI Should Stop Attacking Encryption and Tell Congress About All the Encrypted Phones It's Already Hacking Into. **EFF**, 8 mar. 2021. Disponível em: https://www.eff.org/deeplinks/2021/03/fbi-should-stop-attacking-encryption-and-tell-congress-about-all-encrypted-phones. Acesso em: 01 dez. 2021.

MUNCASTER, Phil. Telegram App Banned in Russia. **Infosecurity**, 16 abr. 2018. Disponível em: https://www.infosecurity-magazine.com/news/telegram-app-banned-in-russia. Acesso em: 29 nov. 2021.

MUNHOZ, Vinicius. WannaCry, o ransomware que fez o mundo chorar na sexta-feira (12). **Tecmundo**, maio 2017. Disponível em: https://www.tecmundo.com.br/malware/116652-wannacry-ransomware-o-mundo-chorar-sexta-feira-12.htm. Acesso em: 10 set. 2021.

NAISA, Letícia. Dos 'salveiros' ao WhatsApp: como o PCC usou a comunicação para se expandir. **Vice**, 17 maio 2016. Disponível em: https://www.vice.com/pt_br/article/ypnmkv/dos-salveirosao-whatsapp-como-o-pcc-usou-as-tecnologias-para-expandir. Acesso em: 18 nov. 2021.

NASCIMENTO, Anderson. O que é a NSA. **Canaltech**, 20 jun. 2014. Disponível em: https://canaltech.com.br/espionagem/O-que-e-a-NSA. Acesso em: 04 nov. 2021.

NEWMAN, Lily Hay. The EARN IT Act Is a Sneak Attack on Encryption: The crypto wars are back in full swing. **Wired**, May 2020. Disponível em: https://www.wired.com/story/earn-it-act-sneak-attack-on-encryption/. Acesso em: 18 out. 2022.

NICAS, Jack. Bitcoin and Encryption: A Race Between Criminals and the F.B.I. **The New York Times**, 12 jun. 2021. Disponível em: https://www.nytimes.com/2021/06/12/technology/fbi-bitcoin-ransom-encryption.html. Acesso em: 01 dez. 2021.

NOGUEIRA, Luiz. Criptografia de ponta a ponta do WhatsApp não é infalível. **Olhar Digital**, 4 nov. 2019. Disponível em: https://olhardigital.com.br/2019/11/04/noticias/criptografia-de-ponta-a-ponta-do-whatsapp-nao-e-infalivel. Acesso em: 30 nov. 2021.

NOGUEIRA, Luiz. WhatsApp revela que agora entrega 100 bilhões de mensagens por dia. **Olhar Digital**, 30 out. 2020. Disponível em: https://olhardigital.com.br/2020/10/30/noticias/whatsapp-agora-entrega-cerca-de-100-bilhoes-de-mensagens-por-dia. Acesso em: 2 dez. 2021.

NUTHI, Kir. The EARN IT Act Would Give Criminal Defendants a Get-Out-of-Jail-Free Card. Disponível em: https://slate.com/technology/2022/02/earn-it-act-fourth-amendment-violation.html. Acesso em: 20 nov. 2022.

OBARRIO, María Carolina; QUINTANA, María. **Mediación Penal**. Buenos Aires: Editorial Quorum, 2004.

OLIVEIRA, Ana Carolina Rezende. Direito, ciência e a racionalidade das premissas empíricas na fórmula do peso de Robert Alexy. In: MARCO, Cristhian Magnus de; BELOTTO, Julian Cristopher; GUSBERTI, Anderson Rodrigo (Org.). **Direitos fundamentais na perspectiva teórica de Robert Alexy**: Tomo VI. Joaçaba: Unoesc, 2016. (Série Direitos Fundamentais Civis). p. 147-170.

OLIVEIRA, João José. WhatsApp libera transferência de dinheiro no Brasil pelo serviço, mas ainda não para todo mundo. **UOL**, São Paulo, 4 maio 2021. Disponível em: https://economia.uol.com.br/noticias/redacao/2021/05/04/whatsapp-vai-permitir-envio-de-dinheiro-para-pessoas-a-partir-de-hoje.htm. Acesso em: 12 dez. 2021.

OLIVEIRA, Larisse Silva. **Diálogos jurisdicionais entre o STF e a Corte Interamericana**: comunicações transjudiciais e jurisprudência internacional de direitos humanos. Belo Horizonte, São Paulo: D'Plácido, 2020.

OLIVEIRA, Wagner Martins Carrasco de. Interceptação telefônica e interceptação telemática como meios tecnológicos no combate à corrupção. In: JORGE, Higor Vinicius Nogueira (Coord.). **Enfrentamento da corrupção e investigação criminal tecnológica**. 2. ed. São Paulo: JusPodivm, 2021.

PAVANELI, Aline. Demora nas perícias de eletrônicos emperra investigações no Paraná; fila para análise passa de 19 mil aparelhos. **G1**, 18 jul. 2018. Disponível em: https://g1.globo.com/pr/parana/noticia/2018/07/18/demora-nas-pericias-de-eletronicos-emperra-investigacoes-no-parana-fila-para-analise-passa-de-19-mil-aparelhos.ghtml. Acesso em: 02 dez. 2021.

PETROV, Daniel. FBI encrypted chat access scorecard ranks iMessage and WhatsApp easy, Telegram hard. **Phone Arena**, 2 dez. 2021. Disponível em: https://www.phonearena.com/news/fbi-encrypted-chat-access-imessage-whatsapp-signal-telegram_id136809. Acesso em: 02 dez. 2021.

PFEFFERKORN, Riana. O debate estadunidense sobre vigilância e criptografia. In: ANTONIALLI, Dennys; ABREU, Jacqueline de Souza (Ed.). **Direitos fundamentais e processo penal na era digital**. São Paulo: InternetLab, 2018. v. 1. p. 108-147. Disponível em: https://congresso.internetlab.org.br/wp-content/uploads/2020/08/Direitos-Fudamentais-e-Processo-Penal-na-era-digital-Volume-1.pdf. Acesso em: 11 nov. 2021.

PFEFFERKORN, Riana. There's now na even worse anti-encryption bill than Earn It. That doesn't make the Earn It bill ok. **CIS**, 24 June 2020. Disponível em: https://cyberlaw.stanford.edu/blog/2020/06/there%E2%80%99s-now-even-worse-anti-encryption-bill-earn-it-doesn%E2%80%99t-make-earn-it-bill-ok. Acesso em: 28 nov. 2021.

PIMENTEL, Fabiano. **Provas, procedimentos e recursos criminais**. Belo Horizonte; São Paulo: D'Plácido, 2020.

POLÍCIA CIENTÍFICA DO PARANÁ. **Relatório estatístico**. 2020. Disponível em: https://www.policiacientifica.pr.gov.br/Pagina/Relatorio-Estatistico. Acesso em: 20 nov. 2022.

PONTAROLLI, André Luis. Política criminal e responsabilidade penal da pessoa jurídica. **Justiça e Sistema Criminal**, Curitiba, v. 10, n. 18, jan./jun. 2018.

PORTNER, Léo. Kann die polizei ihre WhatsApp-, viber- oder Facebook-Nachrichten lesen? **Dr. Miluscheva**. Disponível em: https://www.bg-

anwalt.de/infothek/strafrecht/kann_die_polizei_ihre_whatsapp_viber_oder_facebook_nachrichten_lesen.html. Acesso em: 06 dez. 2021.

POSCHER, Ralf. Resuscitation of a Phantom? On Robert Alexy's Latest Attempt to Save His Concept of Principle. **Ratio Juris**, v. 33, n. 2, p. 134-149, jul. 2020. DOI: https://doi.org/10.1111/raju.12286. Acesso em: 10 out. 2021.

POZEN, David E. The Mosaic Theory, National Security, and the Freedom of Information Act. **The Yale Law Journal**, v. 115, n. 628, 2005, p. 631 e 632. Disponível em: https://core.ac.uk/download/pdf/157778843.pdf. Acesso em: 12 nov. 2021.

PRADO, Geraldo. **A cadeia de custódia da prova no processo penal**. 2. ed. São Paulo: Marcial Pons, 2021.

PRAZERES, Ângela dos; BUSATO, Paulo César. Heterorresponsabilidade e autorresponsabilidade penal de pessoas jurídicas: especial referência ao fato de conexão. In: BUSATO, Paulo César; GRECO, Luís (Coord.). **Responsabilidade penal de pessoas jurídicas**: anais do III seminário Brasil-Alemanha (v. 2, 2019, Berlin). Florianópolis: Tirant lo Blanch, 2020. p. 20-21.

QUITO, Carina. As quebras de sigilo telemático no processo penal e o paradoxo do acesso irrestrito às comunicações armazenadas. In: WOLKART, Erik Navarro et al. (Coord.). **Direito, processo e tecnologia**. 2. ed. São Paulo: Thomson Reuters, 2021. p. 161-186.

RAMIRO, André (Coord.). **O mosaico legislativo da criptografia no Brasil**: uma análise de projetos de lei. Recife**:** IP.Rec, 2020. Disponível em: http://www.obcrypto.org/wp-content/uploads/2020/08/O-mosaico-legislativo-da-criptografia-no-Brasil-uma-an%c3%a1lise-de-Projetos-de-Lei-1.pdf. Acesso em: 26 out. 2022.

RAMOS, João Gualberto Garcez. **Curso de Processo Penal Norte-Americano**. 2. ed. No Prelo.

RAMOS, João Gualberto Garcez. **Curso de Processo Penal Norte-Americano**. São Paulo: Revista dos Tribunais, 2006.

RAMOS, João Gualberto Garcez. **O Devido Processo Legal no Contexto do Processo Penal Adversarial e sua Evolução na Suprema Corte dos EUA**. Goiânia: Lutz, 2022.

REIMAN, Phillip E. Cryptography and the First Amendment: The Right to be Unheard. **Journal of Computer & Information Law**, v. 14, n. 2, p. 325-345, Winter 1996. Disponível em: https://repository.law.uic.edu/cgi/viewcontent.cgi?article=1313&context=jitpl. Acesso em: 18 nov. 2022.

RIBOLI, Eduardo Bolsoni. Eu sei o que vocês fizeram no verão passado": o uso de software de espionagem como meio de obtenção de prova penal. **Revista Brasileira de Ciências Criminais**, São Paulo, v. 156, p. 91-139, jun. 2019.

RICCI, Sergio Diaz. El derecho a la privacidade en la era digital: uma experiência comparada. In: CÉSAR, Joaquim; MEZZETTI, Luca. (Org.). **O direito das novas tecnologias e o ordenamento constitucional**. Belo Horizonte: D'Plácido, 2021.

RILEY, Tonya. The Cybersecurity 202: FBI renews attack on encryption ahead of another possible attack on the Capitol. **The Washington Post**, 4 mar. 2021. Disponível em: https://www.washingtonpost.com/politics/2021/03/04/cybersecurity-202-fbi-renews-attack-encryption-ahead-another-possible-attack-capitol. Acesso em: 01 dez. 2021.

RIPOLLÉS, José Luis Díez. **A racionalidade das leis penais**: teoria e prática. Tradução: Luiz Régis Prado. 2. ed. São Paulo: Revista dos Tribunais, 2016.

ROSENZWEIG, Paul. In Defense of the Mosaic Theory. **Lawfareblog**, Nov. 2019. Disponível em: https://www.lawfareblog.com/defense-mosaic-theory. Acesso em: 08 jul. 2021.

ROSLER, Paul; MAINKA, Christian; SCHWENK, Jörg. More is Less: On the End-to-End Security of Group Chats in Signal, WhatsApp, and Threema. In: IEEE EUROPEAN SYMPOSIUM ON SECURITY AND PRIVACY, 3rd, 2018, London. **Proceedings...** London: EuroS&P, 2018. Disponível em: https://eprint.iacr.org/2017/713.pdf. Acesso em: 30 nov. 2021.

ROXIN, Claus. **Derecho Procesal Penal**. Trad. Castellana de G. Córdoba y D. Pastor. Buenos Aires: Editores del Puerto, 2000.

RPEK, Lucas. How the FBI Is Trying to Break Encryption Without Actually Breaking Encryption. **Gizmodo**, 18 jun. 2021. Disponível em: https://gizmodo.com/how-the-fbi-is-trying-to-break-encryption-without-actua-1847054471/amp. Acesso em: 01 dez. 2021.

SALATIEL, José Renato. Filosofia analítica: Wittgenstein e o argumento da linguagem privada. **UOL**. Disponível em: https://educacao.uol.com.br/disciplinas/filosofia/filosofia-analitica-wittgenstein-e-o-argumento-da-linguagem-privada.amp.htm. Acesso em: 8 jul. 2022.

SANTOS, Tania Steren dos. Globalização e exclusão: a dialética da mundialização do capital. **Sociologias**, Porto Alegre, v. 3, n. 6, p. 170-198, jul./dez. 2001. Disponível em: https://www.scielo.br/j/soc/a/3ZxzcsL7YLskmzn8yLFyCDy/?lang=pt&format=pdf. Acesso em: 17 ago. 2021.

SATO, Gustavo Worcki. A Infiltração Virtual de Agentes e o Combate à Pedopornografia digital. In: JORGE, Higor Vinícius Nogueira (Org.). **Direito Penal sob a Perspectiva da Investigação Criminal Tecnológica**. São Paulo: JusPodivm, 2021. p. 501-512.

SCHÜNEMANN, Bernd. **Estudos de direito penal, direito processual penal e filosofia do direito**. São Paulo: Marcial Pons, 2013.

SEIDEL, Ulrich. **Datenbanken und Persönlichkeitsrecht**: Unter besonderer Berücksichtignung der amerikanichen Computer Privacy. Köhl: O. Schmidt, 1972.

SILVA, Marco Antonio Marques da. Relatório Final do Anteprojeto do Código Penal. **Senado Federal**, Brasília, DF, 12 jun. 2012. Disponível em: https://www.mpma.mp.br/arquivos/CAOPCRIM/Relat%C3%B3rio%20final%20do%20Anteprojeto%20do%20Novo%20C%C3%B3digo%20Penal.pdf. Acesso em: 13 jun. 2021.

SLOBOGIN, Christopher. Making the Most of United States v. Jones in a Surveillance Society: A Statutory Implementation of Mosaic Theory. **Duke Journal of Constitutional Law & Public Policy**, v. 8, p. 1-37, 2012. Disponível em: http://scholarship.law.duke.edu/djclpp/vol8/iss1/1. Acesso em: 07 jun. 2021.

SMENTKOWSKI, Brian P. Fourth Amendment. **Britannica.** Disponível em: https://www.britannica.com/topic/Fourth-Amendment. Acesso em: 22 set. 2021.

SOARES, Gustavo Torres. **Investigação criminal e inovações técnicas e tecnológicas**. Belo Horizonte: D'Plácido. 2020.

SOKOLOV, Andrej. Was die Überwachung der Messenger bedeutet. **WirtschaftsWoche**, Düsseldorf, Juni 2017. Disponível em: https://www.wiwo.de/technologie/digitale-welt/whatsapp-was-die-ueberwachung-der-messenger-bedeutet/19972834.html. Acesso em: 10 set. 2020.

SOPRANA, Paula. Como a polícia pode dar a volta na criptografia do WhatsApp. **Época**, 23 jul. 2016. Disponível em: https://epoca.globo.com/vida/experiencias-digitais/noticia/2016/07/como-policia-pode-dar-volta-na-criptografia-do-whatsapp.html. Acesso em: 12 out. 2021.

SOUZA, Sérgio Ricardo de. **Prova penal e tecnologia**: novas técnicas e meios de investigação e captação de provas. Curitiba: Juruá, 2020.

STATE OF UTAH. Electronic Information or Data Privacy. **Legiscan**, H.B. 57, Mar. 2019. Disponível em: https://legiscan.com/UT/text/HB0057/id/1969570. Acesso em: 05 out. 2021.

STATISTA RESEARCH DEPARTMENT. **Most popular global mobile messenger apps as of October 2021, based on number of monthly active users**. Nov. 2021. Disponível em: https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps. Acesso em: 29 nov. 2021.

SUPREME COURT OF THE UNITED STATES. Carpenter v. United States, 585 U. S. 2018. Disponível em: https://www.supremecourt.gov/opinions/17pdf/16-402_h315.pdf. Acesso em: 07 jul. 2021.

SUPREME COURT OF THE UNITED STATES. Jones v. United States, 132 S. Ct. 945, 2012. Disponível em: https://www.law.cornell.edu/supremecourt/text/10-1259. Acesso em: 7 jun. 2021.

SUPREME COURT OF THE UNITED STATES. Katz v. United States, 389 U.S. 347, 1967. Disponível em: https://supreme.justia.com/cases/federal/us/389/347. Acesso em: 07 jun. 2021.

SUPREME COURT OF THE UNITED STATES. Kyllo v. United States, 533 U.S. 27, 2001. Disponível em: https://supreme.justia.com/cases/federal/us/533/27. Acesso em: 11 nov. 2021.

SUPREME COURT OF THE UNITED STATES. Riley v. California, 573 U.S. 373, 2014. Disponível em: https://supreme.justia.com/cases/federal/us/573/373. Acesso em: 05 jun. 2021.

SYDOW, Spencer Toth. **Curso de direito penal informático**. 2. ed. Salvador: Juspodivm, 2021.

SYMPOSIUM ON SECURITY AND PRIVACY, 3., 2018, London. **Proceedings...** London, 2018. Disponível em: https://eprint.iacr.org/2017/713.pdf. Acesso em: 30 nov. 2021.

TECHOPEDIA. **Encryption Backdoor**. Feb. 2020. Disponível em: https://www.techopedia.com/definition/3743/encryption-backdoor. Acesso em: 30 out. 2021.
TELEGRAM. **Perguntas frequentes**. Disponível em: https://telegram.org/faq?setln=pt-br. Acesso em: 18 nov. 2022.

THAMAY, Rennan; TAMER, Maurício. **Provas do Direito Digital**: conceito da prova digital, procedimentos e provas digitais em espécie. São Paulo. Revista dos Tribunais. 2020.

THE SUPREME COURT – LEADING CASES. Fourth Amendment – Search and Seizure – Searching Cell Phones Incident to Arrest – Riley v. California. **Harvard Law Review**, v. 128, n. 251, p. 251-260, 2014. Disponível em: https://harvardlawreview.org/wp-content/uploads/2014/10/riley_v_california.pdf. Acesso em: 02 nov. 2021.

THE UNITED STATES ATTORNEY'S OFFICE. Department of Justice. U.S. Attorney's Office. FBI's Encrypted Phone Platform Infiltrated Hundreds of Criminal Syndicates; Result is Massive Worldwide Takedown. **Federal Bureau of Investigation**, 8 jun. 2021. Disponível em: https://www.justice.gov/usao-sdca/pr/fbi-s-encrypted-phone-platform-infiltrated-hundreds-criminal-syndicates-result-massive. Acesso em: 26 nov. 2021.

THOMPSON II, Richard M. The Fourth Amendment Third-Party Doctrine. **Congressional Research Service**, June 2014, p. 2.

TRENGOVE, Markus et al. A critical review of the Online Safety Bill. **Patterns**, v. 3, n. 8, Aug. 2022. DOI: https://doi.org/10.1016/j.patter.2022.100544. Acesso em: 17 out. 2022.

TROIS NETO, Paulo Mario Canabarro. Têmis no Divã: fatores Irracionais na ponderação constitucional? In: MARCO, Cristhian Magnus de; BELOTTO, Julian Cristopher; GUSBERTI, Anderson Rodrigo. (Org.). **Direitos fundamentais na perspectiva teórica de Robert Alexy**: Tomo VI. Joaçaba: Unoesc, 2016. (Série Direitos Fundamentais Civis). p. 39-70.

TUDO CELULAR. **WhatsApp tem falha de criptografia que permite manipulação de conversas descoberta**. 2018. Disponível em: https://www.tudocelular.com/seguranca/noticias/n128932/whatsapp-vulnerabilidade-criptografia-descoberta.html. Acesso em: 30 nov. 2021.

UNITED KINGDOM. Department for Digital, Culture, Media & Sport. **Online Safety Bill**. London: DCMS, 2021. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf. Acesso em: 06 dez. 2021.

UNITED KINGDOM. International statement: End-to-end encryption and public safety. **Gov.UK**, Oct. 11 Oct. 2020. Disponível em: https://www.gov.uk/government/publications/international-statement-end-to-end-encryption-and-public-safety/international-statement-end-to-end-encryption-and-public-safety-accessible-version. Acesso em: 15 nov. 2021.

UNITED KINGDOM. Investigatory Powers Act 2016. **UK Legislation**. Disponível em: https://www.legislation.gov.uk/ukpga/2016/25/part/8/chapter/2/crossheading/investigatory-powers-tribunal/enacted. Acesso em: 06 dez. 2021.

UNITED STATES GOVERNMENT. Bureau of Justice Assistance. **The Foreign Intelligence Surveillance Act of 1978 (FISA)**. Disponível em: https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1286. Acesso em: 12 dez. 2021.

UNITED STATES OF AMERICA. Department of Justice. **Cloud Act Resources**. Disponível em: https://www.justice.gov/criminal-oia/cloud-act-resources. Acesso em: 24 nov. 2022.

UNITED STATES OF AMERICA. Department of Justice. **Electronic Communications Privacy Act of 1986 (ECPA)**. Disponível em: https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285. Acesso em 19 set. 2022.

UNITED STATES OF AMERICA. House of Representatives. **Bills & Resolutions**. Disponível em: https://www.house.gov/the-house-explained/the-legislative-process/bills-resolutions. Acesso em: 28 nov. 2021.

UNITED STATES OF AMERICA. House of Representatives. H.R.7891 – Lawful Access to Encrypted Data Act. In: UNITED STATES CONGRESS, 116th, 2019-2020, Washington. **Proceedings...** Washington, 2019-2020. Disponível em: https://www.congress.gov/bill/116th-congress/house-bill/7891/text#toc-H8D2533E6D74E44A2AC049571DCA1C454. Acesso em: 17 out. 2022.

UNITED STATES OF AMERICA. House of Representatives. S.3398 – EARN IT Act of 2020. In: UNITED STATES CONGRESS, 116th, 2019-2020, Washington. **Proceedings...** Washington, 2019-2020b. Disponível em: https://www.congress.gov/bill/116th-congress/senate-bill/3398/text. Acesso em: 11 set. 2020.

UNITED STATES OF AMERICA. Senate. S.4051. Lawful Access to Encrypted Data Act. In: UNITED STATES CONGRESS, 116th, 2019-2020, Washington. **Proceedings...** Washington, 2019-2020. Disponível em: https://www.congress.gov/bill/116th-congress/senate-bill/4051/text. Acesso em: 17 out. 2022.

UNITED STATES. Department of Justice. **Department of Justice's Review of Section 230 of the Communications Decency ACT of 1996**. Disponível em: https://www.justice.gov/archives/ag/department-justice-s-review-section-230-communications-decency-act-1996. Acesso em 19 set. 2022.

UNITED STATES. Microsoft Corporation v. United States of America. Disponível em: https://www.justice.gov/archives/opa/blog-entry/file/937006/download. Acesso em: 20 set. 2022.

UOL. **Brasil é o segundo país no mundo com maior número de crimes cibernéticos**. São Paulo, 15 set. 2018. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2018/02/15/brasil-e-o-segundo-pais-no-mundo-com-maior-numero-de-crimes-ciberneticos.htm. Acesso em: 22 jun. 2021.

VALLEE, Hannah Quay-de la; AZARMI, Mana. The New EARN IT Act Still Threatens Encryption and Child Exploitation Prosecutions. **Center for Democracy & Technology**, 25 Aug. 2020. Disponível em: https://cdt.org/insights/the-new-earn-it-act-still-threatens-encryption-and-child-exploitation-prosecutions. Acesso em: 15 jun. 2021.

VENTURA, Felipe. Proposta quer banir WhatsApp e Telegram se não quebrarem sigilo no Brasil. **Tecnoblog**, 9 jan. 2019. Disponível em: https://tecnoblog.net/274333/whatsapp-telegram. Acesso em: 18 nov. 2021.

VIEIRA, Renato Stanziola. **Controle da prova penal**: obtenção e admissibilidade. São Paulo: Revista dos Tribunais, 2021.

VILARES, Fernanda R. **A Reserva de Jurisdição no processo penal**: dos reflexos no inquérito parlamentar. 2010. 239 f. Dissertação (Mestrado em Direito Processual Penal) – Universidade de São Paulo, São Paulo, 2010. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2137/tde-23112010-

082016/publico/DISSERTACAO_Fernanda_Vilares_239_fls.pdf. Acesso em: 26 out. 2022.

VIVES ANTÓN, Tomás S. **Fundamentos do Sistema Penal**. Tradução: Paulo César Busato. 2. ed. São Paulo: Tirant lo Blanch, 2022.

VIVES ANTÓN, Tomás S. **Pensar la libertad**: últimas reflexiones sobre el derecho y la justicia. Compiladora: María Luia Cuerda Arnau. Valencia: Tirant lo Blach, 2019. p. 625-640.

VOGE, Callum; WILTON, Robin. Internet Impact Brief End-to-end Encryption under the UK's draft Online Safety Bill. **Internet Society**, 5 Jan. 2022. Disponível em: https://www.internetsociety.org/resources/doc/2022/iib-encryption-uk-online-safety-bill/. Acesso em: 14 out. 2022.

VOJTKO, Mark. All About Encryption Backdoors. **The SSL Store**, 18 jan. 2021. Disponível em: https://www.thesslstore.com/blog/all-about-encryption-backdoors. Acesso em: 30 out. 2021.

VOLPATO, Samira. **El Derecho a la Intimidad y las Nuevas Tecnologias de la Información**. 2016. 572 f. Tesis (Doctorado en Derecho Constitucional) – Universidade de Sevilla, Sevilla, 2016. Disponível em: https://idus.us.es/handle/11441/52298. Acesso em: 07 jul. 2021.

WATZMAN, Alyssa; THOMPSON, Bryan. Utah requires warrant or law enforcement access to certain tuypres of data. **Data Privacy & Cybersecurity**, Apr. 2019. Disponível em: https://lewisbrisbois.com/blog/category/data-privacy-cyber-security/utah-requires-warrant-for-law-enforcement-access-to-certain-types-of-data. Acesso em: 12 out. 2021.

WENDT, Emerson; JORGE, Higor Vinícius Nogueira. **Crimes cibernéticos**: ameaças e procedimentos de investigação. Rio de Janeiro: Brasport. 2013.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. Interceptação Telemática de Contas do WhatsApp (bilhetagem – extrato de mensagens) – versão 2019.4. In: JORGE, Higor Vinicius Nogueira (Coord.). **Tratado de Investigação Criminal Tecnológica**. 2. ed. Salvador: JusPodivm. 2021. p. 139-145.
WHATSAPP. **Informações para as autoridades policiais**. Disponível em: https://faq.whatsapp.com/general/security-and-privacy/information-for-law-enforcement-authorities. Acesso em: 30 out. 2022.

WHATSAPP. **Sobre a criptografia de ponta a ponta**. 2021. Disponível em: https://faq.whatsapp.com/general/security-and-privacy/end-to-end-encryption/?lang=pt_br. Acesso em: 30 nov. 2021.

WILLIE, Matt. EARN IT Act lawmaker finally admits the bill is targeting encryption. **Input**, 13 fev. 2022. Disponível em: https://www.inverse.com/input/culture/earn-it-act-lawmaker-admits-bill-is-targeting-encryption. Acesso em: 18 out. 2022.

WILSON, Taylor H. The Mosaic Theory's Two Steps: Surveying Carpenter in the Lower Courts. **Texas Law Review Online**, v. 99, n. 155, p. 156-182, 2021. Disponível em: https://texaslawreview.org/wp-content/uploads/2021/04/Wilson_Final_Read_2-1.pdf. Acesso em 12 nov. 2021.

WILTON, Robin. Encryption myths versus realities of Online Safety Bill - The UK government can't legislate the impossible – a safer society depends on encryption, not breaking it. Disponível em: bit.ly/3uwq6zw. Acesso em: 15 out. 2022.

WITTGENSTEIN, Ludwig. **Tratado lógico-filosófico**. **Investigações Filosóficas**. Tradução e Prefácio: M. S. Lourenço. 6. ed. Lisboa: Fundação Calouste Gulbenkian, 2015.

WOLTER, J. **O inviolável e o intocável no direito processual penal**: reflexões sobre dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal. Organização, introdução e tradução: Luís Greco; tradução: Alaor Leite e Eduardo Viana. São Paulo: Marcial Pons, 2018.

ZANIOLO, Pedro Augusto. **Crimes modernos**: o impacto da tecnologia do direito. 4. ed. Salvador: JusPodivm, 2021.