FACULDADE DE DIREITO DE VITÓRIA
PROGRAMA DE PÓS-GRADUAÇÃO STRICTO SENSU EM DIREITOS E GARANTIAS FUNDAMENTAIS
MESTRADO EM DIREITO

FELIPE AMORIM CASTELLAN

# CRIPTOGRAFIA, DIREITO FUNDAMENTAL À PRIVACIDADE E DEVERES FUNDAMENTAIS DOS PROVEDORES DE MENSAGERIA PRIVADA NA PERSECUÇÃO PENAL

VITÓRIA
2023

FELIPE AMORIM CASTELLAN

# CRIPTOGRAFIA, DIREITO FUNDAMENTAL À PRIVACIDADE E DEVERES FUNDAMENTAIS DOS PROVEDORES DE MENSAGERIA PRIVADA NA PERSECUÇÃO PENAL

Dissertação apresentada ao Programa de Pós-Graduação em Direitos e Garantias Fundamentais da Faculdade de Direito de Vitória, como requisito para obtenção do grau de mestre em Direito.
Orientador: Prof. Dr. Adriano Sant'Ana Pedra

VITÓRIA
2023

FELIPE AMORIM CASTELLAN

# CRIPTOGRAFIA, DIREITO FUNDAMENTAL À PRIVACIDADE E DEVERES FUNDAMENTAIS DOS PROVEDORES DE MENSAGERIA PRIVADA NA PERSECUÇÃO PENAL

Dissertação apresentada ao Programa de Pós-Graduação em Direitos e Garantias Fundamentais da Faculdade de Direito de Vitória, como requisito para obtenção do grau de mestre em Direito.

Aprovada em: 8 de fevereiro de 2023.

COMISSÃO EXAMINADORA

_____

Prof. Dr. Adriano Sant'Ana Pedra
Faculdade de Direito de Vitória
Orientador

_____

Prof. Dr. Américo Bedê Freire Junior
Faculdade de Direito de Vitória

_____

Prof. Dr. Paulo Barrozo
Boston College Law School

_____

Prof. Dr. Cláudio de Oliveira Santos Colnago
Boston College Law School

## AGRADECIMENTOS

Primeiramente a Deus, pois sem ele nada seria possível.

Aos meus pais, Custódio e Olivia, que, pelo exemplo, sempre me ensinaram a importância dos estudos como instrumento de realizações.

À minha esposa, Paula, faço dedicação especial. Mesmo sofrendo as consequências de minha ausência, seu apoio, incentivo e fé, sempre aquilatando as muitas dificuldades de conciliação das obrigações de trabalho, estudo e família, me trouxeram à conclusão desse desafiador trabalho. Sou todo gratidão a você meu amor.

À minha irmã (meu amorzinho), Livia, pela disponibilidade, carinho e revisão do texto, mesmo tendo que deixar em espera importantes demandas próprias.

Aos amigos Olavo e Mauro, que contribuíram para com este trabalho e ao colega, amigo, e parceiro de primeira hora, Hudson, que ladeou comigo os desafios de todo o mestrado, desde os simples trabalho até a escolha do tema desta dissertação.

Ao meu orientador, Adriano Sant`Ana Pedra, por ter estado sempre ao meu lado durante os dois anos do mestrado, período em que fez orientações, críticas, incentivos e apontamentos essenciais para que esta etapa possa ser vencida de maneira exitosa.

Aos demais membros da banca, pela incansável contribuição que ofertam para a evolução para a teoria do direito, bem como por terem aceitado fazer parte de momento tão especial em minha vida.

À Faculdade de Direito de Vitória (FDV), por ter me proporcionado o acesso a conhecimentos jurídicos que sequer imaginava existirem, bem como ter permitido a felicidade de conviver com professores, funcionários e alunos cujos ensinamentos e lembranças levarei para sempre comigo.

## RESUMO

Num cenário fortemente influenciado pelo fenômeno da massificação das comunicações digitais criptografadas, no qual as significativas transformações operadas na vida em sociedade desafiam a capacidade funcional das instituições, esta pesquisa indagou: considerando a essencialidade da criptografia para a concretização de direitos fundamentais, especialmente privacidade e proteção de dados, e ainda os deveres fundamentais dos particulares para com a segurança pública e a administração da justiça, o que pode ser exigido dos provedores de aplicação de mensageria privada criptografada em relação ao cumprimento de decisões judiciais que determinem a interceptação telemática ou a quebra de sigilo de dados? Estabeleceu-se, como objetivo geral, compreender (i) as conexões entre aplicações de mensageria, criptografia, direitos e deveres fundamentais, à luz de questões técnicos e jurídicos que orbitam o (des)cumprimento de decisões judiciais de interceptação telemáticas e de quebra de sigilo de dados estáticos por provedores dessas aplicações, bem como (ii) os reflexos advindos desta complexa interação para a atividade persecutória do Estado. No recorte dos objetivos específicos, buscou-se identificar a evolução do direito fundamental à privacidade, correlacionando-o com a disseminação da criptografia e seus impactos para a persecução penal no contexto da revolução digital e das guerras criptográficas. Ainda, sob corte epistemológico dos paradigmas jurídicos próprios da teoria dos deveres fundamentais e lastreado na essencialidade da criptografia para a sociedade atual, investigaram-se as expectativas constitucionais que recaem sobre os provedores de aplicação de mensageria criptografada no que tange à cooperação com a segurança pública e administração da justiça pelo cumprimento das decisões judiciais de entrega de dados. Por fim, são analisadas as vantagens e desvantagens da busca e obtenção de comunicações armazenadas (backup) e metadados gerados no contexto das diferentes arquiteturas criptográficas em distintas aplicações existentes, sendo delimitados os pressupostos jurídicos de cabimento e abrangência das medidas cautelares probatórias acima citadas. Partiu-se da hipótese inicial de que (i) em relação às interceptações telemáticas, respeitada a arquitetura de cada sistema, tem-se que a criptografia de ponta a ponta inviabiliza, como regra, a interceptação dos dados em fluxo, descabendo, consequentemente, a imposição de sanções por eventuais descumprimentos de decisões judiciais; (ii) em relação à quebra do sigilo de dados digitais estáticos, os provedores de mensageria criptografada deverão viabilizar pronto e adequado acesso às autoridades de persecução penal aos respectivos dados, metadados ou comunicações digitais armazenadas não afetados pela criptografia de que disponham, sempre respeitadas as peculiaridades

técnicas da arquitetura de cada sistema; a recalcitrância injustificada ao cumprimento de decisão abre caminho ao sancionamento, na forma da lei. Como marco teórico, foram utilizadas obras de José Casalta Nabais, com destaque para “O dever fundamental de pagar impostos”, com abordagem dedutiva e procedimento de revisão bibliográfica.

**Palavras-chave**: criptografia; direito fundamental à privacidade; deveres fundamentais; provedor de aplicação de mensageria; persecução penal.

**ABSTRACT**

In a scenario strongly influenced by the phenomenon of massification of encrypted digital communications, in which the significant transformations carried out in life in society challenge the functional capacity of institutions, this research asked: considering the essentiality of encryption for the realization of fundamental rights, especially privacy and protection of data, and also the fundamental duties of individuals towards public security and the administration of justice, which may be required of providers of encrypted private messaging applications in relation to compliance with court decisions that determine telematic interception or breach of data confidentiality? The general objective was to understand (i) the connections between messaging applications, encryption, and fundamental rights and duties in light of technical and legal issues surrounding the (non)compliance with judicial decisions on telematic interception and breach of confidentiality of static data by providers of these applications, as well as (ii) the consequences arising from this complex interaction for the State's persecutory activity. In terms of specific objectives, we sought to identify the evolution of the fundamental right to privacy, correlating it with the dissemination of encryption and its impacts on criminal prosecution in the context of the digital revolution and cryptographic wars. Furthermore, under the epistemological perspective of the legal paradigms typical of the theory of fundamental duties and based on the essentiality of cryptography for today's society, the constitutional expectations that fall on encrypted messaging application providers with regard to cooperation with public security were investigated and administration of justice by complying with court decisions on data delivery. Finally, the advantages and disadvantages of searching for and obtaining stored communications (backup) and metadata generated in the context of different cryptographic architectures in different existing applications are analyzed, and the legal assumptions of appropriateness and scope of the precautionary evidentiary measures mentioned above are defined. The initial hypothesis was that (i) in relation to telematic interceptions, respecting the architecture of each system, end-to-end encryption makes it impossible, as a rule, to intercept data in flow, consequently making it unnecessary to impose sanctions for possible non-compliance with court decisions; (ii) in relation to the breach of the confidentiality of static digital data, providers of encrypted messaging must provide prompt and adequate access to criminal prosecution authorities to the respective data, metadata or stored digital communications not affected by encryption at their disposal, always respecting the technical peculiarities of the architecture of each system; Unjustified recalcitrance in complying with a

decision opens the way to sanctions, in accordance with the law. As a theoretical framework, works by José Casalta Nabais were used, with an emphasis on “The fundamental duty of paying taxes”, with a deductive approach, and a bibliographic review procedure.

**Keywords**: Cryptography; fundamental right to privacy; fundamental duties; messaging application provider; criminal prosecution.

## LISTA DE ABREVIATURAS E SIGLAS

| | | |
|---|---|---|
| ADC | – | Ação Declaratória de Constitucionalidade |
| ADI | – | Ação Direta de Inconstitucionalidade |
| ADPF | – | Arguição de Descumprimento de Preceito Fundamental |
| CNJ | – | Conselho Nacional de Justiça |
| CF | – | Constituição da República Federativa do Brasil de 1988 |
| CPC | – | Código de Processo Civil |
| CPP | – | Código de Processo Penal |
| DF | – | Distrito Federal |
| EUA | – | Estados Unidos da América |
| FBI | – | Departamento Federal de Investigação dos Estados Unidos da América |
| IBGE | – | Instituto Brasileiro de Geografia e Estatística |
| Inq. | – | Inquérito |
| LGPD | – | Lei Geral de Proteção de Dados |
| MCI | – | Marco Civil da Internet |
| MP | – | Medida Provisória |
| ONU | – | Organização das Nações Unidas |
| PL | – | Projeto de Lei |
| STF | – | Supremo Tribunal Federal |
| STJ | – | Superior Tribunal de Justiça |
| TSE | – | Tribunal Superior Eleitoral |
| UNESCO | – | Organização das Nações Unidas para a Educação, a Ciência e a Cultura |

**SUMÁRIO**

**INTRODUÇÃO..... 10**

**1 PRIVACIDADE, PROTEÇÃO DE DADOS, CRIPTOGRAFIA E PERSECUÇÃO PENAL: O ESTADO DA ARTE..... 15**

1.2 BREVES APONTAMENTOS SOBRE A EVOLUÇÃO DA PRIVACIDADE: UM CONCEITO EM TRANSFORMAÇÃO..... 15

1.3 A ERA DA REVOLUÇÃO DIGITAL E A PROTEÇÃO DA PRIVACIDADE..... 20

1.4 O CONTEXTO DA RELAÇÃO ENTRE PROVEDORES DE APLICAÇÃO DE MENSAGERIA, CRIPTOGRAFIA E PERSECUÇÃO PENAL..... 39

1.5 CRIPTOGRAFIA SIMÉTRICA, ASSIMÉTRICA E PONTA A PONTA: CONCEITOS ESSENCIAIS E UTILIDADE..... 44

1.6 GUERRAS CRIPTOGRÁFICAS E DEBATE GOING DARK NO BRASIL E NO MUNDO..... 49

1.7 REGULAÇÃO DA CRIPTOGRAFIA NO BRASIL E OBRIGAÇÃO DE ASSISTÊNCIA DE PROVEDORES DE APLICAÇÃO..... 59

**1.7.1 Tratamento da criptografia no ordenamento jurídico positivo..... 59**

**1.7.2 Obrigação de assistência dos provedores de aplicação..... 61**

**2 CRIPTOGRAFIA, PROVEDORES DE APLICAÇÃO DE MENSAGERIA E TEORIA DOS DEVERES FUNDAMENTAIS NA ERA DIGITAL..... 64**

2.1 DESCUMPRIMENTO DE DECISÕES JUDICIAIS DE INTERCEPTAÇÃO TELEMÁTICA E QUEBRA DE SIGILO DE DADOS E DEVERES FUNDAMENTAIS: UM PANORAMA DE TENSÕES..... 64

2.2 DEVERES FUNDAMENTAIS COMO FERRAMENTA DE EFETIVAÇÃO DE DIREITOS FUNDAMENTAIS..... 69

**2.2.1 Aspectos introdutórios..... 69**

**2.2.2 Dever fundamental de cooperação com a administração da justiça..... 73**

**2.2.3 Dever fundamental de contribuição com a segurança pública..... 74**
2.3 DEVERES FUNDAMENTAIS DOS PROVEDORES DE APLICAÇÃO DE CONTRIBUIR COM A SEGURANÇA PÚBLICA E A COOPERAÇÃO COM A ADMINISTRAÇÃO DA JUSTIÇA..... 75
2.4 A ESSENCIALIDADE DA CRIPTOGRAFIA COMO FERRAMENTA DA PROTEÇÃO DE DADOS: PROBLEMAS E CONSEQUÊNCIAS DE EVENTUAL FLEXIBILIZAÇÃO..... 80
2.5 PARA ALÉM DA METÁFORA DA ESCURIDÃO: AS FORMAS ALTERNATIVAS DE INVESTIGAÇÃO..... 84

**3 FORMAS ALTERNATIVAS DE INVESTIGAÇÃO COMO RESPOSTA POSSÍVEL AO PROBLEMA DA FALTA DE ACESSO AO CONTEÚDO DAS COMUNICAÇÕES ..... 87**
3.1 DADOS EM NUVEM E ANÁLISE DE METADADOS: NOVAS FRONTEIRAS DA PERSECUÇÃO PENAL..... 87
3.2 SERVIÇOS DE NUVENS, BACKUP E ARMAZENAMENTO DE DADOS: VANTAGENS E DESVANTAGENS..... 89
3.3 METADADOS: VANTAGENS E DESVANTAGENS..... 97
3.4 MEDIDAS DE PERSECUÇÃO PENAL PARA ACESSO ÀS COMUNICAÇÕES DIGITAIS: INTERCEPTAÇÃO TELEMÁTICA E QUEBRA DE SIGILO DE DADOS: BREVES COMENTÁRIOS..... 111
3.5 MEIOS COERCITIVOS INDIRETOS PARA COMPELIR O CUMPRIMENTO DO DEVER FUNDAMENTAL DE ENTREGA DE DADOS..... 116

**4 CONSIDERAÇÕES FINAIS..... 118**

**REFERÊNCIAS..... 124**

## INTRODUÇÃO

Mutável por essência, o direito fundamental à privacidade acompanha a realidade da vida em sociedade da antiguidade aos dias de hoje, sendo conformado, dentre outros fatores, pelo estado da arte da tecnologia de cada tempo.

Não por acaso, o fenômeno da digitalização impulsionou significativas transformações na vida das pessoas e na capacidade funcional das instituições sociais e estatais; naturalmente, o direito fundamental à privacidade foi um dos mais impactados e precisou se adaptar para contemplar riscos decorrentes do processamento eletrônico de dados e da vigilância sobre os cidadãos, o que colocou a criptografia em lugar de destaque.

Caracterizada pela "desmaterialização do objeto" (dados e software), pela abertura para as inovações tecnológicas e pela falta de transparência de muitos procedimentos, a revolução digital provocou dificuldades específicas.

Após revelações de Eduard Snowden, ex-funcionário da Agência de Segurança Nacional dos Estados Unidos da América (EUA), em 2013, eclodiu uma forte demanda por privacidade e segurança do usuário nas comunicações on-line, o que impulsionou a disseminação da criptografia forte por padrão em dispositivos e aplicações de comunicação instantâneas presentes na maioria dos smartphones, e trouxe consigo dificuldades específicas às autoridades de inteligência e persecução penal decorrentes das próprias características dessas tecnologias.

Fato é que a tecnologia avançou, as linhas telefônicas perderam importância, as interceptações telefônicas passaram a ser cada vez menos frutíferas e os órgãos de persecução penal se viram diante da necessidade de contar, em diversos cenários, com a colaboração de entidades privadas até então estranhas ao sistema de justiça criminal, as quais, diferentemente das empresas privadas provedoras de serviços de telefonia, não possuíam vínculos jurídicos prévios com o poder público (a exemplo dos contratos de concessão): as Big Techs (dentre elas, os provedores de aplicações de mensageria privadas).

A assimilação da criptografia forte em dispositivos e aplicações, associada ao crescente fenômeno da digitalização dos meios de comunicação, resultaram na exclusão por longos anos

das autoridades de inteligência e persecução penal do acesso ao conteúdo das comunicações privadas, rendendo ensejo a intensas disputas judiciais com grandes corporações de tecnologia, o que se convencionou chamar going dark. O termo designa o fenômeno em que as autoridades públicas, mesmo dispondo de ordem judicial para captar e acessar informações armazenadas e comunicações de algum investigado, não têm a capacidade técnica para isso, representando o começo da fase contemporânea das guerras criptográficas (iniciadas na década de 1990).

Desde o seu nascimento, as cryptowars revelam como a relação entre criptografia e segurança pública é conturbada e, passados mais de 30 anos de embates, uma miríade de argumentos e contra-argumentos já foi vertida nos embates pelos atores neles envolvidos, os quais devem de alguma forma balizar debates mais prescritivos em torno dos problemas surgidos da assimilação da criptografia forte.

As dificuldades relativas ao cumprimento de ordens judiciais destinadas à obtenção e ao acesso de dados digitais em poder de terceiros e a pouca transparência dos procedimentos das aplicações de mensageria fizeram eclodir não só o debate sobre a regulação da criptografia em si, como também sobre a colaboração e responsabilidades dessas companhias para com os órgãos estatais envolvidos na persecução penal. Isso porque a popularização de produtos e serviços digitais passaram a possibilitar o emprego de novas técnicas de investigação com base em dados armazenados em dispositivos eletrônicos individuais ou de grandes corporações (especialmente, no que toca ao escopo deste trabalho, backup em serviços de nuvem e metadados de comunicação).

Em uma perspectiva mais ampla, os desafios em torno do acesso e da utilização dos dados digitais (comunicacionais ou não) são atuais e estão na ordem do dia para as autoridades envolvidas na persecução penal, englobando, dentre outros: (i) os problemas próprios da adoção das tecnologias de segurança da informação (dentre elas, a criptografia), essenciais tanto ao exercício de direitos fundamentais como à proteção de infraestruturas críticas e até mesmo atividades de investigação; (ii) a dificuldade de se obter a colaboração das empresas de tecnologia, mesmo quando ausentes obstáculos técnicos; e (iii) a necessidade de implementação de novas técnicas de investigação como alternativas à falta de acesso ao conteúdo das comunicações. Não bastasse, a obtenção de dados digitais ainda traz um problema adicional, diretamente ligado à sua natureza imaterial, que é (iv) o limite da

jurisdição estatal, já que os dados digitais podem estar alojados em qualquer parte do mundo, não sendo incomum que repousem em provedores situados fora do país onde se dá a investigação. Numa perspectiva mais restritiva, própria deste trabalho, tais aspectos serão analisados dentro do recorte da obtenção e acesso a dados (e metadados) em poder dos provedores de aplicações de mensageria privada.

E como inexistem estruturas estatais regulatórias de vigência global para os serviços na internet, a liberdade de conformação e de organização dos modelos de negócios pelos provedores de aplicações são particularmente amplas, a exigir correlata responsabilidade pelas oportunidades e riscos associados à incorporação das novas tecnologias. Dito de outro modo, é necessário apurar quais são os deveres dos provedores de aplicações, sobretudo no âmbito das comunicações digitais.

A recusa ao cumprimento de decisões por provedores de aplicação de mensageria aparecem como um dos elementos mais recorrentes nas recentes inserções do debate going dark no Brasil e nos Estados Unidos, o que justifica um olhar cuidadoso sobre as situações jurídicas em torno dessas plataformas digitais e das características dos serviços (o que inclui a criptografia) por elas ofertados, sobretudo quando essas questões se encontram submetidas, no caso brasileiro, ao exame do Supremo Tribunal Federal (STF) em diversas ações, inclusive de controle abstrato e concentrado de constitucionalidade – tais como a Arguição de Descumprimento de Preceito Fundamental (ADPF) nº 403, a Ação Direta de Inconstitucionalidade (ADI) nº 57 e a Ação Declaratória de Constitucionalidade (ADC) nº 51.

Hodiernamente, é impróprio considerar as telecomunicações digitais como mero instrumento de troca de comunicação. Trata-se, isso sim, de verdadeira infraestrutura básica quase onipresente, que pode, e será, utilizada para os mais diversos fins, lícitos ou ilícitos. E os aplicativos de mensageria, escopo maior deste trabalho, estão entre as ferramentas digitais com maior penetração na sociedade, estando presentes na quase totalidade dos smartphones conectados à internet, o que revela as oportunidades que daí podem advir para órgãos de persecução a ensejar esta pesquisa acerca das responsabilidades dessas entidades para com a persecução penal.

Ora, se é verdade que os direitos e garantias fundamentais são temas presentes na maioria dos ordenamentos constitucionais ocidentais, onde se estudam suas classificações, características

e conceitos com profundidade; é igualmente verdade que tal não ocorre com os deveres fundamentais, que são deixados em segundo plano apesar da sua relevância na tarefa de efetivação dos princípios e objetivos desses ordenamentos. Nas raras oportunidades em que são lembrados, os deveres fundamentais são comumente associados aos deveres governamentais, e não à responsabilidade da comunidade pelo fato de viver em sociedade.

Com efeito, é impensável idealizar um Estado Democrático de Direito em que não existam deveres fundamentais a serem observados pelos particulares. Por isso, dentro do Programa de Pós-Graduação Stricto Sensu – Mestrado e Doutorado – em Direitos e Garantias Fundamentais da Faculdade de Direito de Vitória (FDV), desenvolveu-se, no âmbito do Grupo de Pesquisa Estado, Democracia Constitucional e Direitos Fundamentais, o conceito de dever fundamental que serve de guia ao presente trabalho: "Dever fundamental é uma categoria jurídico-constitucional, fundada na solidariedade, que impõe condutas proporcionais àqueles submetidos a uma determinada ordem democrática, passíveis ou não de sanção, com a finalidade de promoção de direitos fundamentais". Os deveres fundamentais impõem aos brasileiros natos e naturalizados, aos estrangeiros que no Brasil se encontrem, bem como às pessoas jurídicas nacionais ou estrangeiras que no território brasileiro desempenham suas atividades, a observância de padrões de conduta pautados na solidariedade e que se voltem para que todas as pessoas possam desfrutar de uma vida digna, nos moldes em que garantido pelo art. 1º, III, da Constituição Federal (CF) de 1988.

É desse cenário que extraímos a importância de investigar se, ao lado dos direitos fundamentais viabilizados pela criptografia, existem deveres fundamentais em jogo que devam ser sopesados, mormente quando se observa que os dispositivos e princípios constitucionais atinentes à segurança pública e à administração da justiça oferecem proteção a vários outros direitos fundamentais.

Posto este cenário, cabe indagar: considerando a essencialidade da criptografia para a concretização de direitos fundamentais, especialmente privacidade e proteção de dados, e ainda os deveres fundamentais dos particulares para com a segurança pública e a administração da justiça, o que pode ser exigido dos provedores de aplicação de mensageria privada criptografada em relação ao cumprimento de decisões judiciais que determinem a interceptação telemática ou a quebra de sigilo de dados?

À luz desses questionamentos centrais, o presente trabalho tem como objetivos: (i) no primeiro capítulo, identificar a evolução do direito à privacidade, correlacionando-o com a disseminação da criptografia e os impactos daí advindos para a persecução penal no contexto da revolução digital e das guerras criptográficas; (ii) no segundo capítulo, sob corte epistemológico dos paradigmas jurídicos próprios da teoria dos deveres fundamentais e baseado na premissa da essencialidade da criptografia na sociedade atual, verificar se os provedores de aplicação de mensageria têm deveres, qualificados como fundamentais, para com a segurança pública e a administração da justiça; e (iii) no terceiro capítulo, a partir da apresentação de algumas técnicas alternativas de investigação digital e dos pressupostos jurídicos de sua incidência, apontar formas de os provedores de aplicação de mensageria se desincumbirem dos seus deveres fundamentais, e expor, ao final, medidas de coerção indireta à disposição do Poder Judiciário para coagir tais provedores ao cumprimento de seus deveres.

Para tanto, o presente trabalho faz uso do método dedutivo, mediante pesquisa bibliográfica, legislativa e de relatórios de pesquisa como fontes-base de conceitos e entendimentos essenciais, visando à construção de conhecimento adequado para promover análise crítica quanto ao tema escolhido. São também usadas fontes secundárias, como jurisprudências, artigos jornalísticos de veículos de comunicação respeitados, livros e artigos sobre as questões trazidas neste estudo.

Com base no caminho percorrido ao longo dos três referidos capítulos, a hipótese inicial é que: (i) em relação às interceptações telemáticas, respeitada a arquitetura de cada sistema, tem-se que a criptografia de ponta a ponta inviabiliza, como regra, a interceptação do fluxo das comunicações, descabendo, consequentemente, a imposição de sanções por eventuais descumprimentos de decisões judiciais; (ii) em relação à quebra do sigilo de dados estáticos, os provedores de mensageria criptografada deverão viabilizar pronto e adequado acesso às autoridades de persecução penal aos respectivos dados, metadados ou comunicações digitais armazenadas não afetados pela criptografia de que disponham, sempre respeitadas as peculiaridades técnicas da arquitetura de cada sistema. A recalcitrância injustificada ao cumprimento de decisão abre caminho ao sancionamento, na forma da lei.

# 1 PRIVACIDADE, PROTEÇÃO DE DADOS, CRIPTOGRAFIA E PERSECUÇÃO PENAL: O ESTADO DA ARTE

Antes de se avançar às problematizações centrais do presente trabalho, cumpre, inicialmente, tecer algumas considerações acerca da evolução do conceito de privacidade a partir de alguns marcos temporais especialmente relevantes à contextualização dos impactos que as tecnologias produzem sobre a sociedade.

## 1.2 BREVES APONTAMENTOS SOBRE A EVOLUÇÃO DA PRIVACIDADE: UM CONCEITO EM TRANSFORMAÇÃO

Jürgen Habermas reconhece, na cultura da Grécia antiga, a origem das categorias público e privado, as quais, afirma o autor, foram repassadas posteriormente à tradição romana. Ensina que, na cidade-estado desenvolvida, a esfera da pólis era identificada como âmbito daquilo que dizia respeito a todos os cidadãos livres (koiné). A esfera da pólis era dissociada da esfera do oikos (casa, em grego), representativa do que era particular a cada indivíduo (idion). Nas palavras do filósofo e sociólogo alemão, "[...] a esfera privada está ligada à casa não só pelo nome; possuir bens móveis e dispor de força de trabalho tampouco constituem substitutivos para o poder sobre a economia doméstica e a família [...]. A posição na pólis baseia-se, portanto, na posição de déspota doméstico" (Habermas, 2003, p. 13-14).

Hannah Arendt corrobora a visão de Habermas ao identificar na política e na família a raiz da distinção entre esfera pública e privada na antiguidade grega. Pontua, outrossim, existir clara autonomia entre as noções, porquanto, para cuidar das relações com o mundo, era indispensável que o cidadão fosse, no mínimo, senhor de um lugar seu (Arendt, 2020).

No curso da Idade Média, não é possível visualizar, com clareza, emanações do desejo de isolamento das pessoas. Quando muito, é possível notar que alguns poucos indivíduos dispunham de meios para obter o afastamento, a exemplo dos senhores feudais que desejassem realizar refeições distantes dos seus empregados. Afora tais privilegiados, monges, bandidos, místicos e eremitas também compunham o restrito grupo de interessados em obter o isolamento (Doneda, 2020).

Cotejando a realidade econômica e social decorrente da desagregação da sociedade feudal verificada na Idade Média, pontua Stefano Rododà que, naquele período, emergiu uma maior preocupação com a privacidade, principalmente com o objetivo de encobrir hábitos sexuais, fisiológicos ou mesmo religiosos (Rodotá, 2008). O isolamento, antes reservado a um reduzido número de indivíduos, passou a ser alcançado por qualquer pessoa que dispusesse de meios materiais para tanto. E foi exatamente com os avanços das técnicas de construção e arquitetura das habitações que o distanciamento entre os indivíduos se tornou possível, continuando, todavia, reservado a poucos privilegiados.

Acresça-se que a exigência de condições materiais e de fortuna mantiveram a classe operária fora do horizonte do direito à privacidade no contexto das revoluções industriais, revelando a feição proprietária do instituto, enquanto direito tipicamente burguês. Segundo Stefano Rodotà (2008, p. 26.27):

> [...] Basta lembrar os dados coletados por Engels sobre a situação habitacional dos operários ingleses em Londres, Edimburgo, Bradfors, Leeds e Manchester, para perceber, pelo contraste, as conotações elitistas do conceito de privacidade. Foi dito acertadamente que 'poverty and privacy are 15el et cobtradictoires': aliás, o 'direito de ser deixado só' pode assumir um significado imensamente negativo quando isso implica no desinteresse pelas condições de vida dos menos favorecidos, representando o abandono do mais fracos à violência social (grifo nosso).

A ideia de privacidade orientada pelo direito de propriedade perdura, grosso modo, até o final do século XIX, quando então emergem novas alterações na dinâmica da vida em sociedade impulsionadas grandemente pelas inovações dos meios de comunicação e da informação, notadamente o jornal impresso e as máquinas fotográficas (Doneda, 2020).

A par dos períodos históricos pinçados, é certo que foi com Samuel D. Warren e Luis Brandeis (este posteriormente alçado à condição de Juiz da Suprema Corte Americana), os "pais fundadores" da privacidade no campo jurídico (Rodotà, 2008), que o direito à privacidade ganhou contornos mais concretos, passando a ser compreendido como direito a ser deixado em paz, de não ser incomodado ou de estar só (Brandeis; Warren, 1890). Sob esta ótica, a privacidade se desgarra do direito de propriedade e se aproxima de uma tutela voltada à proteção da personalidade. Assevera Danilo Cesar Maganhoto Doneda (2020, p. 127):

> Direito a ser deixado em 'paz' ou, para alguns, 'direito a estar só'. O right to be let alone, enunciado pelo magistrado norte-americano Cooley ao final do século passado, foi um dos alicerces do célebre artigo de Brandeis e Warren, The right to privacy. O estudo foi pioneiro ao estabelecer um marco na doutrina do direito à

> privacidade, além de ser de certa forma profético ao antecipar a importância que a matéria viria a assumir com o desenvolvimento das tecnologias de informação que começam a se fazer sentir.

O artigo “The right to privacy”, referência praticamente unânime nos trabalhos acerca do tema, foi confeccionado a quatro mãos e publicado pela dupla em 1890. A publicação foi muito influenciada pela exposição não autorizada em jornais de fatos íntimos relacionados ao casamento da filha de Samuel Warren (Doneda, 2021). Assim consignaram os autores:

> Recentes invasões e métodos negociais chamam a atenção para o próximo passo que deve ser dado com vistas à proteção da pessoa e para a segurança do indivíduo, aquilo que o juiz Cooley chama de ´o direito a ser deixado em paz´. Fotografias instantâneas e empresas jornalísticas invadiram o espaço sagrado da vida doméstica, e numerosos aparelhos mecânicos ameaçam tornar realidade o vaticínio de que ´o que é sussurrado nos quartos há de ser proclamado aos quatro ventos´ (tradução livre) (Brandeis; Warren, 1890, p. 195).

Com efeito, bem se vê que a noção de privacidade é conformada em atenção aos aspectos culturais, sociais, políticos e econômicos de cada tempo. Exatamente por isso que a evolução das tecnologias e os impactos que elas produzem na vida em sociedade são relevante combustível propulsor das transformações da privacidade ao longo da história.

Seguindo a toada evolutiva, o direito à privacidade, até então calcado na exclusão contra interferências alheias, de marcante viés individualista e elitista, começa a receber novos aportes a partir das tecnologias surgidas nos pós segunda guerra mundial. Depois das primeiras décadas do século XX, a demanda sempre crescente por informação e a ampliação das suas formas de difusão seguiram em evolução no encalço do desenvolvimento das novas tecnologias, ao que se seguiu o proporcional aumento das possibilidades de processamento e utilização dessas informações. Esse movimento se dissipou ao redor do mundo, notabilizando-se por deflagrar uma série de reações legislativas e debates jurisprudenciais, sobretudo nos Estados Unidos e na Europa, tendo a Alemanha ocupado especial papel vanguardista, já na década de 1970 (proteção da privacidade a partir da tutela das informações e dados pessoais).

É desse contexto que emerge a relevância das informações pessoais, compreendidas como toda sorte de informação que se refira a uma pessoa. Se é verdade que as informações pessoais interessam tanto a organismos públicos como privados, com justificativa no incremento do controle e da eficiência de seus projetos, é igualmente certo que, na marcha da história, foi o Estado o primeiro a dispor de meios de processar e utilizar informações

pessoais em grande escala. O motivo é singelo: por longo período, os organismos públicos dispuseram de primazia na obtenção de meios computacionais e de coleta de informação em relação à iniciativa privada, confrontada com os elevados custos decorrentes dessas atividades.

Marco inquestionável desse estado de coisas, referenciado em todas as obras sobre proteção de informações e dados pessoais, é a decisão da Corte Constitucional alemã, no idos de 1983, sobre o processo de recenseamento daquela nação. A Lei do Censo (de 1982) possibilitava ao Estado alemão o cruzamento de informações obtidas mediante questionário (com 160 questões) acerca das profissões, das residências e dos locais de trabalho daquele povo, entre outras questões. O pano de fundo do acórdão da Corte foram os reflexos produzidos pela evolução tecnológica sobre o processamento eletrônico de dados, até então desconhecidos, e que gerou muito desconforto e desconfiança dos alemães.

Tendo como premissa a consolidação de um direito geral da personalidade (de caráter abstrato e aberto, para permitir novos desdobramentos de proteção do indivíduo) (Mendes, 2020, p. 10), o Tribunal Constitucional consignou na fundamentação do emblemático acórdão, em apertada síntese, que: (i) "[...] não existem mais dados insignificantes no contexto do processamento eletrônico de dados" (Martins, 2005, p. 244-245); (ii) com o processamento eletrônico, o poder de decisão acerca do fornecimento de dados a terceiros restaria comprometido diante da possibilidade de formulação de perfis de personalidade sem que o interessado pudesse controlar e influir no processo ou no uso dos dados, o que, em última instância, malferiria a própria democracia, fundada na capacidade de ação e participação dos cidadãos; (iii) "[...] o livre desenvolvimento da personalidade pressupõe, sob as modernas condições do processamento de dados, a proteção do indivíduo contra levantamento, armazenagem, uso e transmissão irrestritos de seus dados pessoais" (Martins, 2005, p. 237); (iv) desse direito (de índole fundamental) de proteção decorre o "[...] poder do cidadão de determinar em princípio ele mesmo sobre a exibição e o uso de seus dados pessoais" (Martins, 2005, p. 238), que se especifica como direito à autodeterminação informativa; (v) o direito à autodeterminação informativa não é ilimitado, porquanto a informação e os dados relativos às pessoas representam "[...] recorte da realidade social que não pode ser associado exclusivamente ao indivíduo atingido, haja vista a importância que a estatística desempenha na política governamental (por causa da demanda de informações do Estado ou de terceiros)", razão pela qual o "[...] indivíduo tem que aceitar limitações de seu direito à autodeterminação

sobre a informação em favor do interesse geral predominante" (Martins, 2005, p. 238); (vi) essas limitações, contudo, devem ter assento constitucional e devem atender ao "[...] princípio da clareza normativa do Estado de direito", devendo o legislador atentar nessa regulamentação ao princípio da proporcionalidade, eis que é da essência dos direitos fundamentais que sua limitação só pode ocorrer "[...] pelo poder público quando isso for imprescindível para proteção de interesses públicos"; (vii) tendo em vista os enormes riscos do processamento eletrônico de dados, impõe-se ao legislador que tome "[...] precauções organizacionais e processuais que combatam o perigo de uma violação do direito da personalidade"; (viii) a "[...] obrigação de fornecer dados pessoais pressupõe que o legislador defina a finalidade de uso por área e de forma precisa, e que os dados sejam adequados e necessários para essa finalidade", sendo inadmissível o armazenamento de "[...] dados não anônimos, para fins indeterminados ou ainda indetermináveis" (Martins, 2005, p. 40); e (ix) somente o anonimato e a garantia de sigilo dos dados estatísticos autorizam seu compartilhamento com outros órgãos públicos para desempenho das tarefas de planejamento, sem o que não é exigível do cidadão a disponibilização dos seus dados (Martins, 2005, p. 243).

A fundamentação acima sintetizada exalta preocupação ainda atual, e constitui marco jurisprudencial internacional acerca da proteção de dados pessoais, dando projeção a um novo direito, o de autodeterminação informativa. A Decisão do Censo de 1983 constitui verdadeiro divisor de águas justamente por extrair do direito geral de livre desenvolvimento da personalidade um direito à autodeterminação informativa, à vista das modernas condições de processamento de dados.

Esse novo direito confere, em síntese, proteção ao cidadão contra o acesso, o armazenamento, a utilização e a transmissão não autorizada de dados pessoais, porquanto centram no indivíduo, em princípio, o poder de decidir sobre entrega e uso de seus dados pessoais. Dado seu caráter relativo, o poder de controle sobre os dados pessoais pode ser limitado quando confrontado com interesse público de assento constitucional, desde que haja intermediação legislativa que, a um só tempo, atenda ao princípio da proporcionalidade na tarefa de regulamentação da intervenção e contemple precauções e procedimentos que minimizem os riscos decorrentes das possibilidades de processamento eletrônico de dados. A partir das balizas fixadas no julgado, é possível antever que o poder de controle sobre os próprios dados poderia sofrer restrições quando confrontados com os interesses coletivos de maior

envergadura, como a eficiência na investigação e repressão da criminalidade e medidas de incremento da segurança pública. Na mesma quadra, Freire Júnior e Senna (2009) asseveram que uma real adequação do Direito e do Processo Penal é imprescindível num contexto em que o Estado deve tutelar não somente direitos e garantias individuais do investigado/réu contra possíveis abusos, porquanto é fundamental que se alcance maiores níveis de efetividade na prevenção e repressão frente à complexidade da criminalidade moderna.

A jurisprudência do Tribunal Constitucional reverberou em solo brasileiro e, como se verá adiante, são inúmeras as semelhanças com o julgamento da ADI 6387, ajuizada contra as disposições da Medida Provisória (MP) nº 954.

Retomando, o célebre e histórico julgado da Corte Constitucional alemã marca um momento a partir do qual a temática da privacidade passa a se voltar, cada vez mais, às informações e, principalmente, aos dados pessoais.

Ocorre que, com a revolução 4.0, as informações e os dados pessoais assumiram proeminência inédita. Profundas transformações se operam na vida em sociedade e o próprio sistema capitalista é impactado e modificado substancialmente. Os reflexos também são percebidos na própria atividade persecutória do Estado. Por também receberem os efeitos concretos da revolução digital, as autoridades de persecução precisam compreender a inteireza dos fenômenos que atingem suas atividades para que, assim, possam se adaptar com a maior eficiência possível e não perder as oportunidades associadas às incorporações das inovações. Imprescindível, para tanto, que se conheçam alguns traços da revolução digital e seus impactos sobre a proteção da privacidade.

## 1.2 A ERA DA REVOLUÇÃO DIGITAL E A PROTEÇÃO DA PRIVACIDADE

O fenômeno da globalização e o discurso da sociedade de risco encerram uma significativa modificação do panorama da sociedade contemporânea, sobretudo se atentarmos para as transformações proporcionadas pelo desenvolvimento tecnológico, a exigir franca e veloz adaptação do indivíduo e da própria coletividade.

Deve ficar claro, desde logo, que é a tecnologia a nota elementar impulsionadora da necessidade de adaptação do comportamento humano nas mais diversas áreas de sua atuação (família, trabalho, lazer, relações com o Estado, ciências, entre outras).

Foi a partir do fim do século passado e o início do presente que tais transformações se tornaram mais perceptíveis, porquanto os notáveis avanços nas áreas de inteligência artificial, robótica, cibernética, biotecnologia, informática, neurociência, realidade virtual e nanotecnologia passaram a permear as mais variadas formas da vivência humana, seja no âmbito das relações interpessoais ou na interação das pessoas com o mundo (aí compreendido o virtual).

Os impactos foram, são e continuarão sendo superlativos em todos os campos da vida e do conhecimento humano. Naturalmente, com o direito não poderia ser diferente.

Revolução 4.0 (revolução da internet ou revolução digital), fundada na inteligência artificial[1] e na internet das coisas (Morais, 2018, p. 884), é o termo utilizado para designar as intensas transformações concentradas no início do presente século, por ocasião do uso massivo da internet, aplicativos, smartphones, redes sociais e toda sorte de máquinas inteligentes que modificaram a forma como o indivíduo vive, consome, trabalha, socializa-se ou realiza negócios jurídicos para satisfazer suas necessidades.

Com José Luis Bolzan de Morais, podemos afirmar que os impactos da revolução 4.0 são permanentemente renovados e impulsionados pela velocidade das transformações, em uma aceleração contínua do tempo (Morais, 2021), o que, cada vez mais, exige um amplo poder de adaptação do direito à nova realidade posta. Não é difícil notar que a própria (e clássica) dicotomia entre o que é público e o que é privado vem se liquefazendo de forma (ainda mais) assombrosa com a revolução da internet.

Se é verdade que em períodos históricos pretéritos o comércio fomentou, em certa medida, a diminuição do isolamento entre os grupamentos sociais, elevando o reduzido volume de troca

[1] Segundo José Luis Bolzan de Morais (2018, p. 884), "[...] inteligência artificial (IA) significa dotar computadores e softwares de capacidade para processar imensos volumes de dados e – principalmente – para encontrar padrões e fazer previsões sem ter sido programados para tanto, produzindo dados a partir de dados, ou metadados, aptos a produzir conhecimentos específicos baseados em padrões e comportamentos, bem como realizar controles".

de informações entre eles como efeito positivo das negociações, igualmente verdadeiro é o fato de que as limitações dos modais de transporte e dos meios de comunicação confinavam o câmbio intercultural a poucos indivíduos. Basicamente mercadores e pessoas abastadas eram dotados de poder econômico suficiente para custear viagens longas e, com isso, obter acesso à informação, disso decorrendo uma quase exclusividade do acesso à informação (que acabava por circular muito pouco).

Com o passar do tempo, as atividades comerciais entre os povos se intensificaram. Novas tecnologias surgiram e trouxeram desenvolvimento para os meios de comunicação e transportes até o ponto em que conhecemos atualmente. Hoje, os meios de transporte têm o poder de levar o indivíduo, fisicamente, de um lado a outro do globo (ou mesmo para fora do planeta) em curto espaço de tempo.

Todavia, ainda assim, nada se compara aos ganhos em termos de velocidade de comunicação e processamento de dados. Reuniões virtuais entre pessoas que se encontram fisicamente em continentes distintos e a possibilidade de entabular as mais variadas transações (locações de imóveis, compra de ativos financeiros, aquisição de produtos e serviços, por exemplo) ao redor do globo ressignificam os horizontes do fenômeno da globalização como até então era entendido. Mais que isso, a tecnologia conectou permanentemente Estados, culturas e pessoas por meio do intercâmbio de dados e informações entre os envolvidos, rendendo ensejo a uma verdadeira democratização em larga escala do acesso à informação.

Em que pese o panorama retratado não seja dotado de homogeneidade global, não é menos verdade que a revolução da internet acabou por entrelaçar aquilo que correntemente era entendido por esfera privada e pública, produzindo verdadeira simbiose entre essas noções. Com apenas um comando, imagens e textos produzidos na intimidade do lar ganham o alcance global por intermédio das redes sociais, provocando toda sorte de reações e emoções naqueles que visualizam tais postagens. A própria socialização antes verificada nos espaços públicos das cidades hoje se volta para um espaço público global, qual seja, a internet.

Nas palavras de Carlos Eduardo Malinowski, “[...] com a internet o espaço público já não é mais a cidade, não é mais a região, Estado, nem mesmo a nação, mas o próprio globo, o que permite universalizar as relações privadas e públicas” (Malinowski *et al*, 2020, p. 77). Surgem os óculos de realidade virtual e as interações sociais digitais são cada vez mais utilizadas. O

número de redes sociais se eleva, assim como o de aplicações de comunicação, e as plataformas de jogos on-line também passam a integrar o complexo cenário das comunicações on-line, tudo isso em dispositivos móveis que podemos trazer conosco, no bolso, em qualquer lugar. E não é só. Pessoas mal-intencionadas detêm o poder de romper, a distância, a privacidade por meio da invasão e assunção do controle de dispositivos que armazenam nossos dados, intentando obter algum tipo vantagem.

É nesse espaço público global que uma enormidade de dados é coletada, processada e devolvida aos usuários na forma de publicidade. Aqui se vê uma das marcas características do capitalismo cognitivo ou de vigilância[2], desencadeado pela revolução da internet e que tem nos dados a sua principal mercadoria. Shoshana Zuboff preleciona que, nessa modalidade de capitalismo, os interesses se voltam não mais para as reais necessidades dos indivíduos, mas sim para a predição de comportamentos orientada à maximização dos lucros. Esclarece Zuboff (2019b):

> A velha reciprocidade entre as empresas e os usuários desaparece por trás do projeto de extrair excedentes de nosso comportamento para fins concebidos por outros – vender publicidade. Nós não somos mais os sujeitos da realização do valor. Também não somos, como alguns já afirmaram, o "produto" vendido pelo Google. Somos os objetos cuja matéria é extraída, expropriada e em seguida injetada nas usinas de inteligência artificial do Google, as quais fabricam os produtos preditivos que são vendidos a clientes reais – as empresas que pagam para jogar nos novos mercados comportamentais.

Sendo a informação a matéria-prima do capitalismo de vigilância, emerge a existência de dois tipos de mercados de informações pessoais, a saber: o primário e o secundário. O traço distintivo entre as modalidades alinha-se com a existência ou não de permissão para a coleta de informações por parte do interessado. Assim aduz Stefano Rodotà:

> [...] um mercado 'primário', no qual se trocam informações cedidas consensualmente pelo interessado, com ou sem contrapartidas e com todos os limites que, como foi já lembrando, acompanham a manifestação do consentimento nessa e em outras matérias; e um mercado 'secundário', no qual circulam informações coletadas à

[2] Segundo Shoshana Zuboff: "O capitalismo de vigilância reivindica de maneira unilateral a experiência humana como matéria-prima gratuita para a tradução em dados comportamentais. Embora alguns desses dados sejam aplicados para o aprimoramento de produtos e serviços, o restante é declarado como superávit comportamental do proprietário, alimentando avançados processos de fabricação conhecidos como "inteligência de máquina" e manufaturado em produtos de predição que antecipam o que um determinado indivíduo faria agora, daqui a pouco e mais tarde. Por fim, esses produtos de predições são comercializados num novo tipo de mercado para predições comportamentais que chamo de mercados de comportamentos futuros. Os capitalistas de vigilância têm acumulado uma riqueza enorme a partir dessas operações comerciais, uma vez que muitas companhias estão ávidas para apostar no nosso comportamento futuro" (grifo da autora) (ZUBOFF, 2019a).

> revelia do interessado, ou então utilizadas para finalidades que ele ignora (Rodotá, 2008, p. 133)[3]

A captação, o tratamento e o uso de dados sem consentimento do usuário são uma preocupação decorrente da revolução 4.0, estampada corriqueiramente em reportagens acerca de grandes vazamentos de dados de usuários de plataformas digitais na rede mundial de computadores.[4] Por todos, cabe rememorar a obtenção indevida (e mundialmente noticiada) pela Cambridge Analytica de informações de milhões de usuários do Facebook para traçar o perfil de eleitores nas eleições presidenciais norte-americanas.[5]

Acontecimentos desse gênero tendem a ser tornar cada vez mais normais, porquanto ainda não se estabeleceram instrumentos normativos dotados de eficácia social suficiente para pautar o comportamento dos conglomerados tecnológicos no ciberespaço e estabelecer adequadamente suas responsabilidades, muito embora avanços venham ocorrendo em todo o mundo.

Esse estado de coisas é animado pelo valor inato que as informações pessoais assumem na nova roupagem do capitalismo, tudo a exigir uma redefinição não só da proteção à privacidade (que deve ir além do direito a ser deixado só), como também dos instrumentos jurídicos de tutela. Os poderes constituídos também não podem ficar de fora do debate, porquanto não há dúvidas de que serão continuamente chamados a examinar demandas veiculando pretensões atinentes ao uso, controle e tratamento de dados. É exatamente nesse cenário que nascem as criptoguerras, delas advindos valiosos aportes necessários à compreensão da relação entre criptografia, direitos e deveres fundamentais, persecução penal e (des)cumprimento de decisões judiciais de entrega de dados.

Firmada a fundamentalidade constitucional da inafastabilidade da jurisdição (acesso à justiça) em caso de lesão ou ameaça a direito (art. 5º, XXXV, CF), é inegável que o sistema de justiça será sempre um dos palcos finais onde serão travadas as mais intensas disputas em torno da

---

[3] Shoshana Zuboff segue no mesmo sentido e assevera: "O capitalismo de vigilância precisa trabalhar com ambos os lados da equação. De um lado, suas tecnologias são projetadas para converter nossa experiência em dados, como o óleo a partir da gordura. Isso costuma ocorrer sem a nossa consciência, muito menos o nosso consentimento. Do outro lado da equação, toda vez que encontramos uma interface digital tornamos a nossa experiência passível de 'dataficação', portanto, 'entregamos ao capitalismo de vigilância' a contribuição contínua de suprimento de matéria-prima" (ZUBOFF, 2019a).

[4] A propósito, ver: https://computerworld.com.br/sem-categoria/os-10-vazamentos-de-dados-maisassustadores-que-aconteceram-em-2018/. Acesso em: 4 jul. 2021.

[5] Sobre o assunto, ver: https://g1.globo.com/economia/tecnologia/noticia/2019/01/09/cambridgeanalytica-se-declara-culpada-por-uso-de-dados-do-facebook.ghtml. Acesso em: 4 jul. 2021.

temática de privacidade e da proteção de dados pessoais, seja na esfera cível ou penal. Concebido como instrumento voltado à tutela dos bens jurídicos mais caros à sociedade, o direito penal não passa ao largo das modificações proporcionadas pelos avanços tecnológicos, notadamente em se considerando a ampliação dos espaços e métodos de atuação das autoridades que investigam e punem criminosos.

Igualmente, a disciplina processual penal deve permanecer antenada às implicações probatórias advindas dos avanços da digitalização e diminuição dos ambientes analógicos. Compreender como se desenvolvem algumas das intrincadas relações entre privacidade, proteção de dados pessoais, segurança da informação e interesse coletivo de eficiência estatal na investigação e punição de crimes é exigência de primeira hora aos que pretendam lançar um olhar atento aos desafios da persecução penal na era digital. Sem essa compreensão, fica impossível extrair respostas idôneas e alternativas factíveis aos problemas e desacordos que se colocam.

De rigor, assim, que se compreenda adequadamente o que se entende por privacidade e proteção de dados, seus espaços de proteção e limites.

## 1.3 PRIVACIDADE, PROTEÇÃO DE DADOS E AUTODETERMINAÇÃO INFORMATIVA: CONTEÚDO E CONFORMAÇÃO NORMATIVA

Numa primeira aproximação, pode-se associar a privacidade às normas de bloqueio que se destinam a assegurar ao indivíduo a existência de espaços livres de interferência alheia, o que oferece suporte à feição liberal e democrática do direito em tela. Nesse sentido (Doneda; Machado, 2019, p. 47):

> A privacidade compõe-se de um conjunto de normas de bloqueio, porque asseguradoras de inviolabilidades. Ela fundamenta a licitude de espaços de não interferência juridicamente tutelados. Trata-se de característica típica de estados liberais e das democracias espelhadas em seus valores. O direito à privacidade implica, por isso, liberdades e imunidades oponíveis a priori contra investidas de terceiros, notadamente o Estado (mas não apenas ele), dentro dos espaços por ela tutelados.

No plano jurídico internacional, a Declaração dos Direitos do Homem e do Cidadão de 1948 trouxe, em seu artigo 12, que “[...] ninguém será sujeito à interferência na sua vida privada, na

sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação [...]" (Brasil, 1945).

O Pacto Internacional de Direitos Civis e Políticos, incorporado ao ordenamento nacional pelo Decreto nº 592, de 6 de julho de 1992, estabelece semelhante proteção ao prever, em seu artigo 17, que "[...] ninguém será objecto de ingerências arbitrárias ou ilegais na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem de ataques ilegais à sua honra e reputação" (Brasil. 1992).

O Pacto de San José da Costa Rica não destoa dos documentos internacionais anteriores, dispondo em seu artigo 11 que "[...] ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação" (Brasil, 1992).

Entre nós, o direito à privacidade esteve presente em todas as constituições brasileiras, apresentando-se, porém, sob a rubrica da inviolabilidade do domicílio e das correspondências. Cuidando da inviolabilidade dos direitos civis e políticos, já a Constituição do Império de 1824 (Brasil, 1824) previa, em seu artigo 179, a inviolabilidade do domicílio nos seguintes termos: "[...] todo o cidadão tem em sua casa um asilo inviolável. De noite, não se poderá entrar nela, senão por seu consentimento, ou para o defender de incêndio, ou inundação; e de dia só será franqueada a sua entrada nos casos, e pela maneira que a Lei determinar". A inviolabilidade das correspondências era assegurada nos seguintes termos: "[...] segredo das cartas é inviolável. A administração do correio fica rigorosamente responsável por qualquer infração deste artigo". Registre-se que esses direitos constam, com adaptações, em todas as constituições que se seguiram.

A partir dos dispositivos da Carta do Império transcritos, verifica-se a feição proprietária da privacidade na primeira constituição brasileira, o que é compatível com aquela quadra da história. Recorde-se que foi apenas em 1890 que Samuel D. Warren e Luis Brandeis publicaram seu célebre artigo, dando início à ruptura da conexão entre privacidade e o direito de propriedade.

No âmbito do direito positivo interno e vigente, a Constituição da República de 1988 cuidou, desde sua concepção, da matéria em múltiplos dispositivos ao longo do texto e, de forma mais

específica, no inciso X do artigo 5º, assim dispondo (Brasil, 1988): “[...] são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”. Estabeleceu, ainda, ser “[...] inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal” (art. 5º, XII, CF). Registre-se, desde logo, que a constitucionalização da proteção de dados, de maneira expressa no texto constitucional, só veio no ano de 2022, o que será melhor detalhado adiante.

Veja-se que não há previsão da palavra privacidade no texto constitucional. Igualmente, o Código Civil nada prevê acerca do termo privacidade, limitando-se a afirmar que “[...] a vida privada da pessoa natural é inviolável” (Brasil, 2002).

Cotejando as disposições citadas, bem como a imensa dificuldade de se fornecer um conceito unitário à privacidade, Marcel Leonardi coloca que esse é um desafio doutrinário que repercute em todo o mundo, havendo inclusive quem aponte ser impossível delimitar completamente o que seria privacidade. Outros, ainda mais descrentes, posicionam-se pela inutilidade da busca pela definição de vida privada. Fato é, todavia, que, no âmbito das visões unitárias de privacidade, merecem destaque os conceitos de privacidade como “[...] direito a ser deixado só, direito ao resguardo contra interferências alheias, direito ao segredo, direito ao sigilo e direito de controlar as informações e dados pessoais” (Leonardi, 2012, p. 46).

Não bastasse a dificuldade conceitual, impende considerar, ainda, que o texto constitucional traz duas expressões distintas no dispositivo de regência, quais sejam, intimidade e vida privada. Diante da dualidade de termos empregados, emergiram respeitáveis posicionamentos defendendo que vida privada e intimidade se distinguiriam quanto ao conteúdo. A vida privada seria uma concepção mais ampla, enquanto a intimidade representaria um aspecto mais interno e intenso da privacidade (Lafer, 1988; Ferraz Júnior, 1993), abarcando o segredo e a confidência. Noutro giro, há quem defenda que a Constituição foi redundante, não havendo utilidade na diferenciação (Leonardi, 2012).

Em que pese não se desconhecer a máxima hermenêutica de que a lei não traz palavras inúteis, é forçoso reconhecer que tal distinção não possui importância prática diante da

inviolabilidade garantida pelo texto constitucional. Nesse particular, estamos com José Afonso da Silva (2009, p. 208), que prefere utilizar o termo privacidade em sentido genérico e amplo, a abarcar, em seu conteúdo, todas as manifestações da esfera íntima, privada e da personalidade, trazidas pela Constituição:

> [...] a terminologia não é precisa. Por isso, preferimos usar a expressão direito à privacidade, num sentido genérico e amplo, de modo a abarcar todas essas manifestações da esfera íntima, privada e da personalidade, que o texto constitucional em exame consagrou. Toma-se, pois, a privacidade como o conjunto de informação acerca do indivíduo que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições, sem a isso poder ser legalmente sujeito. A esfera de inviolabilidade, assim, é ampla, abrange o modo de vida doméstico, nas relações familiares e afetivas em geral, fatos, hábitos, local, nome, imagem, pensamentos, segredos, e, bem assim, as origens e planos futuros do indivíduo.

Fixada a preferência pelo termo privacidade, cumpre consignar o seu conceito, o que fazemos nos valendo dos ensinamentos de Stéfano Rodotà, para quem o direito à privacidade pode ser definido como "[...] o direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir a sua própria esfera particular" (Rodotà, 2008, p. 15). Esfera particular essa que deve ser compreendida como "[...] conjunto de ações, comportamentos, opiniões, preferências, informações pessoais, sobre as quais o interessado pretende manter um controle exclusivo" (Rodotà, 2008, p. 92). Em outras palavras, o direito à privacidade é o direito de manter o controle: conhecer, endereçar, interromper o fluxo, controlar as formas de circulação das próprias informações.

Justifica-se a adoção do conceito funcional tendo por base, principalmente, as diversas transformações e preocupações (sempre crescentes) decorrentes dos

avanços das tecnologias da informação e da comunicação, de modo que o direito à privacidade não pode mais ser estruturado como "pessoa-informação-segredo", mostrando-se hoje muito mais produtivo compreendê-lo segundo o eixo "pessoainformação-circulação-controle" (Rodotà, 2008, p. 92). Nas palavras do multicitado autor italiano: "A tecnologia ajuda a moldar uma esfera privada mais rica, porém mais frágil, cada vez mais exposta a ameaças: daí deriva a necessidade de fortalecimento contínuo de sua proteção jurídica, da ampliação das fronteiras do direito à privacidade" (Rodotà, 2008, p. 95).

A necessidade de ressignificação do direito à privacidade [6] também ecoou na doutrina nacional. A nova perspectiva é assimilada, dentre outros, por André Ramos Tavares[7] e por José Adércio Sampaio. Nas palavras de José Adércio Sampaio (2013):

> Ainda que autorizada a captação, a pessoa ainda detém o direito de controlar o uso das informações pessoais que não se contém no âmbito do domínio fático dessas informações, de sua exclusividade, próprios do conceito de "segredo", mas vai além: ainda quando as informações tenham saído desses domínios, a pessoa – de que se trata – continua a exercer um "controle" sobre sua destinação. Vale dizer que não poderão ser usadas: armazenadas, processadas, tratadas, comunicadas, transmitidas, divulgadas ou publicadas – sem que tenha sido inequivocamente dada a autorização para tanto. Mais uma vez estamos a falar de um controle normativo e não natural. Informação pessoal não pode ser entendida como "segredo" ou como "informação confidencial", senão como, literalmente, "informação a respeito de uma pessoa". Ou de maneira mais clara: informações que tornem a pessoa identificada ou identificável.

Como se vê, Tércio Sampaio Ferraz Jr. foi feliz ao correlacionar, em seu clássico, o princípio da privacidade com regras específicas da proteção de dados e das comunicações, o que foi objeto de acolhida por parte da Corte Constitucional brasileira. Ferraz propôs, em suma, que a privacidade fosse vista em níveis distintos de "exclusividade" sobre aquilo que o indivíduo deseja expor ao escrutínio de terceiros, sendo que os espaços de exposição podem ser mais públicos ou mais restritos, chegando, inclusive, ao domínio dos segredos da intimidade. Pela leitura que se faz do autor, nota-se que a privacidade seria um direito marcado pela complexidade, haja vista ser integrado por diversos direitos subjetivos, como o nome e a imagem (que pressupõem, para sua tutela, a apresentação do indivíduo às relações sociais), e o direito ao sigilo, consistente na faculdade de ficar ausente da esfera pública, isso é, ficar recluso do convívio alheio.

Confinar o direito à privacidade ao direito de estar só, hodiernamente, equivaleria a subestimar a sua relevância frente aos impactos da revolução 4.0. Como sustenta José Adércio Sampaio (1998, p. 495):

---

[6] Registre-se, com Freire Júnior, que a própria "complexidade do mundo moderno favorece a concepção relativista de direitos fundamentais". E prossegue asseverando que é vã a pretensão que objetive argumentar a existência, em abstrato, de um núcleo essencial dos direitos fundamentais, haja vista que a noção mesma de essencialidade pode facilmente se dissipar quando confrontada com casos concretos. (FREIRE JÚNIOR, 2015. p. 60-61).

[7] Nas palavras do insigne doutrinar: "Pelo direito à privacidade, apenas ao titular compete a escolha de divulgar ou não seu conjunto de dados individuais, e, no caso de divulgação, decidir quando, como, onde e a quem. Os dados em questão são todos aqueles que decorram da vida familiar, doméstica ou particular do cidadão, envolvendo fatos, atos, hábitos, pensamentos, segredos, atitudes e planos de vida" (TAVARES, 2006, p. 579.)

> A total transparência do indivíduo ante aos olhos do Estado e das empresas, detentores de monopólio de informação, agudiza a concentração de poder, fragiliza o controle que deve ser exercido pela sociedade - e não, sobre a sociedade - e tende a aprofundar a desigualdade de suas relações, favorecendo as discriminações e o conformismo social e político, assim como a ´ditadura do simulacro´. [...] Fala-se de uma nova categoria de excluídos: os exclus de l´abstratcion. A intimidade ascende de um valor burguês a um valor democrático essencial.

Não há como negar que o direito à proteção de dados pessoais representa uma précondição para o gozo de outros direitos igualmente fundamentais. Forçoso reconhecer que sem uma firme proteção aos dados e informações pessoais, o cidadão fica vulnerável a discriminações de toda sorte, sejam lastreadas em suas crenças religiosas, alinhamentos políticos, sindicais ou associativos, ou mesmo por conta de suas condições de saúde. Para além de a proteção da privacidade se configurar como traço garantidor da igualdade e da liberdade constitucionalmente estabelecidas, ela assume, ainda, a feição de força opositora à construção de uma sociedade da vigilância, onde as pessoas são selecionadas e classificadas conforme as informações que delas se extraem.

O conceito funcional adotado, orientado pela valorização do controle sobre os dados e informações pessoais, leva especialmente em consideração o plexo de transformações que a tecnologia proporcionou em nossa existência, sobretudo a partir da 2ª Guerra Mundial (com a evolução do processamento automatizado de dados), até chegar aos dias atuais, marcados pela influência exercida pela revolução 4.0 (ou revolução da internet).

O conceito de privacidade, centrado no controle do indivíduo sobre os seus dados pessoais, reverberou no reconhecimento de uma especificação do respectivo direito fundamental, desbordando no reconhecimento do direito à autodeterminação informativa, caracterizado pelo poder de o indivíduo decidir quando, se e dentro de quais limites é possível o uso, o tratamento e a circulação dos seus dados pessoais.

Mesmo antes da Emenda Constitucional nº 115, já era possível divisar os claros contornos do direito fundamental em análise, não só pela decorrência da proteção constitucional da privacidade, como também da tutela jurídica dos dados cristalizada no artigo 5º, inciso XII, que dispõe ser "[...] inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas [...]" (Brasil, 1988) (grifo nosso). Some-se que o reconhecimento da fundamentalidade do direito à autodeterminação informativa emerge da forte proteção constitucional manifestada na cláusula geral de tutela da personalidade e da

promoção humana, valor-fonte da ordem jurídica constitucional que traz como um de seus fundamentos a dignidade da pessoa humana (Bioni, 2019).

Acresça-se que a adoção da privacidade como garantia de controle, e cristalizada como autodeterminação informativa, permite enxergar com clareza, a um só passo, a tutela de um amplo feixe de direitos e valores de índole constitucional. Consubstanciase em proteção do valor liberdade (artigo 5º, caput, da CF) na medida em que coloca nas mãos do titular a aferição autônoma do quanto daquilo que lhe diz respeito será (se é que será) exposto à esfera de terceiros, ou mesmo a organizações públicas e privadas; o valor igualdade ganha contornos concretos porquanto se agudiza a premissa de que informações e dados pessoais que denotem opiniões, crenças religiosas, estilo de vida, filiação a organizações sindicais, políticas e filosóficas, e preferências de toda sorte, só chegarão ao conhecimento de terceiros mediante consentimento do seu titular, evitando-se que se convertam em elemento de discriminação ou estigmatização social[8].

Também a cidadania e a democracia são reforçadas, haja vista que a garantia de controle sobre os dados pessoais corrige a estrutura assimétrica (geradora de conflitos) do poder baseado em dados, retirando do mercado e de organismos públicos o uso e a manipulação irrestritos e devolvendo tal poder aos reais titulares, incrementando o espírito democrático, afinal "Todo o poder emana do povo [...]" (artigo 1º, caput, inciso II e parágrafo único, da CF). Ainda, a proteção dos dados pessoais importa em franco reforço à tutela da liberdade de expressão e de comunicação (quando abriga de violação os dados sobre opiniões pessoais) e da liberdade religiosa e de associação (dados sobre vida religiosa e associativa, respectivamente).

Em suma, o que se pode perceber é que a proteção de dados se afigura como précondição para o gozo e escorreita fruição de inúmeros direitos igualmente marcados pela nota da fundamentalidade constitucional. Nas palavras de Stefano Rodotà (2008, p. 236):

[8] Segundo Stefano Rodotà: "Não há dúvida de que o conhecimento, por parte do empregador ou de uma companhia seguradora, de informações sobre uma pessoa infectada pelo HIV, ou que apresente características genéticas particulares, pode gerar discriminações. Estas podem assumir a forma da demissão, da não admissão, da recusa em estipular um contrato de seguro, da solicitação de um prêmio de seguro especialmente elevado" (RODOTÀ, 2008, p. 70). E ainda pontua o multicitado autor italiano: "[…] coletar dados sensíveis e perfis sociais e individuais pode levar à discriminação; logo, a privacidade deve ser vista como 'a proteção de escolhas de vida contra qualquer forma de controle público e estigma social' (L. M. Friedman), como a 'reivindicação dos limites que protegem o direito de cada indivíduo a não ser simplificado, objetivado, e avaliado fora de contexto' (J. Rosen)" (RODOTÀ, 2008, p. 15).

> [...] Uma forte tutela dos dados sensíveis tornou-se componente essencial da igualdade para evitar a coleta destas informações específicas possa se transformar em instrumento de discriminação da pessoa. Mas a tutela de dados sanitários ou genéticos é também a condição para realizar o direito à saúde, assim como a tutela dos dados sobre as opiniões pessoais torna-se premissa para o exercício das liberdades de expressão, de comunicação, de associação, de culto. E a condição de trabalhador, o acesso ao crédito e aos seguros, dependem cada vez mais da intensidade da tutela das informações pessoais.

A proteção de dados é, pois, a disciplina herdeira da garantia da privacidade em tempos de processamento eletrônico de dados, de decisões automatizadas adotadas com base em dados pessoais, de vazamentos de dados e invasões a dispositivos eletrônicos. Nessa ordem de ideias, verifica-se que privacidade e segurança do cidadão andam de mãos dadas na era digital (Doneda, 2020, p. 60):

> A análise integrada das questões aqui apresentadas faz transparecer que "privacidade" e "segurança" caminham lado a lado, não o contrário. Se a violação da privacidade impacta no conjunto de direitos humanos, um dos mais afetados é sem dúvida o direito à segurança. Compromete-se inclusive a segurança nacional, se considerada a prática de vigilância de um Estado sobre o outro.

David Kaye, Relator Especial da Organização das Nações Unidas (ONU) para a liberdade de expressão, corrobora a conexão existente entre privacidade e segurança coletiva. Reflete que não há dúvida de que a massificação das tecnologias da comunicação e da informação faz da segurança on-line (proteção de dados) uma exigência de primeira ordem para todos. Para sua garantia, a criptografia assume especial relevância, eis que fornece “[...] a indivíduos e grupos uma zona de privacidade online para manter opiniões e exercer a liberdade de expressão sem interferências arbitrárias e ilegais ou ataques”, viabilizando, ainda, que “[...] indivíduos sejam capazes de verificar se suas comunicações são recebidas apenas por seus destinatários pretendidos, sem interferência ou alteração, e que as comunicações recebidas são igualmente livres de intrusão” (ASSEMBLEIA, 2017, p. 198-199).

Entre nós, e mesmo antes da Lei Geral de Proteção de Dados ganhar corpo, tramitava no Congresso o Projeto de Emenda Constitucional nº 17/2019, o qual objetivava inserir a proteção de dados pessoais no rol de direitos fundamentais positivados, o que foi muito motivado à vista de relevantes decisões da Suprema Corte brasileira acerca da proteção de dados pessoais, da privacidade e dos direitos fundamentais. Concluído o processo legislativo especial, o indigitado Projeto recebeu a aprovação das casas legislativas, rendendo ensejo à publicação da Emenda Constitucional nº 115/2022, responsável por incluir o inciso LXXIX

ao artigo 5º da Constituição Federal. Assim foi que, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais, foi formalmente constitucionalizado no título II da Constituição, referente aos direitos e garantias fundamentais.

A despeito de o Brasil positivar o reconhecimento da fundamentalidade do direito à proteção de dados pessoais apenas em 2022, é importante destacar que na Europa isso se deu há algumas décadas. O Tratado de Lisboa, em vigor desde 2009, projetou a proteção de dados pessoais à condição de direito fundamental no artigo 8º da Carta dos Direitos Fundamentais da União Europeia, ao lado do direito à privacidade (artigo 7º), reverberando a marca da fundamentalidade (de há muito) sedimentada na cultura alemã, de certa forma pioneira nesse particular aspecto, ainda que em sede de jurisdição constitucional.

Sob essa ótica, é viável concluir que a inserção do inciso LXXIX no artigo 5º da Constituição Federal brasileira assume contornos de uma especial valorização do enfoque constitucional do tratamento de dados pessoais, haja vista que, tornando inequívoca a fundamentalidade da proteção dos dados, termina por, ao menos no plano teórico, elevar as expectativas constitucionais sobre as responsabilidades reservadas àqueles que guardam, usam, tratam e transmitam esses dados.

É evidente que os direitos fundamentais são concebidos, principalmente, como direitos de defesa dos seus titulares contra a intervenção do Estado, inclusive sob o ângulo das revoluções do passado. Tem-se, com Pedra (2018), que a liberdade individual se ergue como valor supremo, devendo ser assegurada sobretudo pela abstenção de intervenção do Estado sobre relações da comunidade, especificando-se sob a nomenclatura de liberdade negativa. Em sua dimensão substancial, os direitos fundamentais se apresentam como prerrogativas indispensáveis para a garantia de vida digna dos cidadãos. Em sua dimensão formal, os direitos fundamentais correspondem à base sobre a qual se devem estruturar todos os demais direitos, emprestando-lhes fundamento, e sem eles não se pode exercer muitos outros. Dito de outro modo, os direitos fundamentais estão garantidos pela Constituição, que é a fonte primeira de origem e validade de todas as normas que criam ou garantem os demais direitos (Pedra, 2018).

Descendo ao plano infraconstitucional, o direito à autodeterminação informativa foi expressamente consagrado na Lei nº 13.709, de 13 de agosto de 2018, denominada Lei Geral

de Proteção de Dados (LGPD), como fundamento da disciplina da proteção de dados pessoais. A reprodução de alguns de seus dispositivos permite bom panorama da norma em comento:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.
> Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
> [...]
> Art. 5º Para os fins desta Lei, considera-se:
> [...]
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> [...]
> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
> [...]
> XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
> [...]
> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de
> dados [...] (Brasil, 2018).

Cumpre asseverar que após as revelações de Snowden o Brasil esteve na vanguarda de uma coalizão global de promoção do direito à privacidade (Sshulz, 2016). O Marco Civil da Internet (MCI) recebeu tramitação diferenciada para que o Poder Legislativo pudesse dar rápida resposta às preocupações surgidas do escândalo de vigilância. O Brasil foi reconhecido como um dos primeiros países a introduzir uma lei ampla com o objetivo de disciplinar, em um único pacote normativo, as regras de uso da internet. Muito embora a liberdade de expressão e a privacidade já estivessem tuteladas pela Constituição brasileira, o Marco Civil explicitou que esses direitos também devem ser garantidos no ambiente on-line, além, é claro, de prever uma série de relevantes princípios, a exemplo da neutralidade da rede (Schulz; Van

Hoboken, 2016). A preocupação específica com a proteção da privacidade e dos dados aparece na Lei nº 12.965, de 23 de abril de 2014, com clareza meridiana:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei
> [...]
> 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, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
> 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
> [...]
> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei (Brasil, 2014).

Como já asseverado, no plano internacional, a Carta de Direitos Fundamentais da União Europeia contemplou, em artigos distintos, a diferenciação entre o direito "ao respeito pela vida privada e familiar" (art. 7º) e o "direito à proteção de dados de caráter pessoal" (art. 8º). A densidade das disposições, separando a privacidade da proteção de dados, denota, a um só tempo, não só a fundamentalidade dos direitos tratados, como também deixa antever certa autonomia entre eles, o que, segundo Stéfano Rodotà, pode ser considerado o último ponto da longa evolução do conceito de privacidade (Rodotà, 2008, p. 16).

Mesmo antes da edição da citada Carta de Direitos Fundamentais, a Diretiva Europeia nº 95/46/CE determinava a adoção de normas de proteção de dados pessoais (tratamento e circulação) aos diversos países do bloco, condicionando "[...] o ingresso no Acordo de Schengen – o que permite a livre circulação dos cidadãos no território europeu – à existência da lei nacional e ao efetivo funcionamento da autoridade" (Moraes, 2021).

Como já salientado, a jurisprudência paradigmática da Corte Constitucional alemã reverberou em solo brasileiro e, como se verá adiante, são inúmeras as semelhanças com o julgamento da ADI 6387, ajuizada contra as disposições da MP 954/2020.

Em 17 de abril de 2020, foi editada a MP 954, que tratou do compartilhamento de dados por empresas de telecomunicação prestadoras de serviço telefônico com o Instituto Brasileiro de

Geografia e Estatística (IBGE), para fins de suporte à produção estatística durante a pandemia do coronavírus (covid-19). A Medida Provisória previu o dever das empresas de telefonia fixa e móvel de disponibilizar ao IBGE, em meio eletrônico, a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas (art. 2º). Essas informações serviriam, nos termos da MP, para a realização de entrevistas não presenciais com os consumidores, em face da realidade de isolamento social imposta pela covid-19 (Brasil. 2020).

Contra a Medida Provisória foram, então, ajuizadas cinco ações diretas de inconstitucionalidade (reunidas sob a rubrica da ADI 6387) (Brasil, 2020). Afirmou-se, em síntese, que haveria inconstitucionalidade formal (ausência de relevância e urgência indispensáveis para a edição do instrumento normativo) e que as disposições da MP importariam em violação à intimidade, à vida privada, à honra e à imagem das pessoas, ao sigilo de dados pessoais e à autodeterminação informativa. A eficácia da MP acabou sendo suspensa após o deferimento de medida cautelar, ad referendum do Plenário da Suprema Corte, pela Ministra Rosa Weber. A cautelar foi referendada em 7 de maio de 2020, mantendo-se a suspensão da MP 954/2020, contudo, ante a sua não conversão em lei, decidiu-se pela perda superveniente do objeto das ações diretas, extinguindo-se o processo objetivo de controle de constitucionalidade sem exame do mérito. Não obstante, remanesce a importância paradigmática dos fundamentos que levaram à concessão da medida cautelar. Senão vejamos.

Os principais fundamentos utilizadas para se decidir pela inconstitucionalidade da MP 954/2020 podem assim ser sintetizados: (i) ausência de previsão de mecanismos técnicos de proteção e segurança dos dados pessoais contra acessos não autorizados, vazamentos acidentais ou utilização indevida, a fazer presente proteção insuficiente dos direitos fundamentais em jogo (mormente pela falta de previsão de cuidados para a anonimização ou pseudominização dos dados pessoais); (ii) ausência de delimitação acerca do objeto, da finalidade e da amplitude da estatística a ser produzida, o que faz com que não seja possível avaliar a adequação e necessidade da MP, assim entendidas como a compatibilidade do tratamento com as finalidades informadas e sua limitação ao mínimo necessário para alcançar suas finalidades; (iii) violação ao Regulamento Sanitário Internacional (RSI 2005 – incorporado e promulgado pelo Decreto nº 10.212, de 30 de janeiro de 2020), que estabelece critérios rígidos para tratamento de dados pessoais quando relevantes para a tutela da saúde pública, que só devem ocorrer quando adequados, relevantes e não excessivos em relação a

esse propósito e conservados apenas pelo tempo necessário (artigo 45, § 2º, alíneas “b” e “d”); (iv) ao prever o compartilhamento de dados de milhões de usuários, a MP incorre em excesso, pois as pesquisas amostrais do IBGE envolvem, em média, apenas cerca de 70 mil domicílios por mês; e (iv) indevida a disposição que preconiza a confecção de impacto à proteção de dados seja elaborada somente após a realização do compartilhamento.

Preocupação fortemente manifestada ao longo dos votos foi a possibilidade de formação de perfis com dados como nome, endereço e telefone, quando conjugados com as entrevistas. Essa união poderia gerar níveis alarmantes de precisão na identificação dos usuários dos serviços de telefonia, a denotar a total transparência do indivíduo aos olhos do Estado, bem como renderia ensejo à possibilidade de criação de “[...] ‘filter bubbles’, ou seja, bolhas de filtros, onde se pode identificar a tendência das pessoas, quer dizer, a invasão vai mais do que a privacidade, a invasão chega mesmo à esfera da própria liberdade intrínseca do pensamento”, nas palavras do Ministro Luiz Fux (Brasil, 2020).

Em último esforço de síntese, o que nos parece ser o ponto nevrálgico da decisão foi a falta de transparência da MP em delimitar adequadamente objetivos, métodos, segurança e procedimentos que envolveriam o compartilhamento dos dados, o que justificaria a intervenção no direito fundamental à autodeterminação informativa dos seus titulares frente ao dever de proteção da saúde pública que justificaria a produção estatística. Dito de outro modo, a MP malferiria a proporcionalidade, em suas vertentes adequação e necessidade, também denominados subprincípios ou máximas parciais.

Por tudo que se viu até aqui, pode-se afirmar, com segurança, que é o direito à privacidade que fundamenta a licitude dos espaços e serviços destinados à promoção e ao resguardo do indivíduo a das informações que a ele se referem. Os direitos e deveres correspondentes existirão não apenas para os potenciais violadores desses espaços, como também para os que possuam o “[...] dever legal ou contratual de protegê-los – sejam agentes públicos, por força de lei, sejam privados, por determinação legal ou contratual”[67].

Evidenciada a premissa da fundamentalidade do direito à autodeterminação informativa, antes ou depois da Emenda Constitucional 115, resta concluir que esse direito, como qualquer outro, não é absoluto, podendo ceder em sua aplicação frente a interesses preponderantes. Indigitada intervenção no direito fundamental em comento carece, contudo, de justificativa,

firme e concreta, eis que “[...] quanto mais intensiva é uma intervenção em um direito fundamental tanto mais graves devem ser as razões que a justificam”. No mesmo sentido, Pedra preleciona que não obstante a Constituição Federal trazer de maneira solene os direitos fundamentais, eles não são compreendidos como absolutos, pois podem estar sujeitos a certos limites (Alexy, 1999, p. 78).

Não se pode olvidar, ademais, que os direitos fundamentais, assim como as demais normas constitucionais, não compõem uma realidade estanque, presa aos ideais e projetos dos legisladores/constituintes (que lhes forneceram legitimidade democrática) ou confinada nos limites da literalidade do texto escrito. É sobremaneira essencial que cada sociedade possa projetar a constituição, senão o próprio direito, conforme certas balizas do seu tempo (Pedra, 2018), sem necessidade de, a todo momento, socorrer-se do devido processo legislativo. É por esse motivo que se considera, em princípio, particularmente útil que as normas que tratem de direitos fundamentais sejam interpretadas numa perspectiva evolutiva e dinâmica ao longo do tempo, sem descurar, contudo, de que algumas premissas importantes permaneçam hígidas mesmo diante da realidade em constante transformação (Hoffmann, 2022).

No âmbito do Supremo Tribunal Federal, não são raros os exemplos de decisões que analisaram a aplicação dos direitos fundamentais ante as mudanças proporcionados por novas tecnologias, tal qual se deu com os direitos ao sigilo bancário, fiscal e telefônico (Brasil, 2000).

Se, por um lado, é auspicioso constatar que a interpretação dos direitos fundamentais deve acompanhar as transformações sociais e culturais sem nunca abandonar seu caráter de proteção do cidadão, por outro, é viável observar que uma visão extremada dessa perspectiva poderia incorrer em excessos e deixar desprotegidos outros valores igualmente constitucionais. No item que se segue, essa perspectiva será contextualizada a partir de um problema concreto do nosso tempo, que é a proteção das comunicações privadas por meio da criptografia e os seus consequentes impactos sobre a atividade persecutória do Estado, legitimado único do direito/dever de punir com penas corpóreas.

## 1.4 O CONTEXTO DA RELAÇÃO ENTRE PROVEDORES DE APLICAÇÃO DE MENSAGERIA, CRIPTOGRAFIA E PERSECUÇÃO PENAL

Com efeito, o moderno contexto de circulação de dados e informações entre pessoas fez surgir a necessidade de se implementarem mecanismos de segurança da informação nas comunicações travadas mediante conexão com a rede mundial de computadores.

Em que pese o principiar do fenômeno da digitalização remonte há várias décadas, é certo que ele só ganhou impulso ao final da década de 1990. Foi com o enorme crescimento do número de usuários e aplicações da internet ao longo da primeira década deste século que se verificaram os concretos efeitos do veloz avanço no progresso tecnológico sobre vida das pessoas e na capacidade funcional das instituições sociais e estatais (Hoffmann, 2022, p. 10). Anota Hoffmann-Riem que "[...] a desmaterialização do objeto – dados e software –, a abertura para o futuro do desenvolvimento tecnológico, e a falta de transparência de muitos procedimentos (black boxes) provocam dificuldades específicas" (Hoffmann, 2022, p. 10).

Além da proliferação das plataformas de compartilhamento de dados e redes sociais (o que foi denominado Web 2.0, por agregar a interatividade do usuário na produção de conteúdo disponível na internet), outra inovação que marcou a primeira década do século XXI foi o surgimento dos smartphones, verdadeiros computadores portáteis.
Carlos Liguori (2022, p. 132) assevera que:

> Outra relevante inovação surgida na década de 2000 foi o smartphone – telefones celulares conectados à Internet que possuem funcionalidades quase idênticas a de um computador pessoal. As múltiplas funcionalidades (além da praticidade) providas pelo dispositivo tornaram-no a principal forma de acesso à Internet nos dias de hoje. Smartphones são ricas fontes de dados sobre seus usuários, abrangendo tanto informações pessoais como profissionais. Apesar de conveniente, a concentração de tantas informações em um único dispositivo é algo bastante alarmante do ponto de vista da cibersegurança.

A tecnologia evoluiu, os métodos de comunicação avançaram e, com isso, as linhas telefônicas tiveram sua importância significativamente reduzida. Os smartphones viabilizaram novas formas de comunicação instantâneas e com custo baixo (por vezes, sem custo) por intermédio de aplicações conectadas à internet. Com tais aplicações, viu-se a incorporação de importantes tecnologias destinadas à proteção da segurança do usuário, dentre elas, a criptografia.

A criptografia pode ser definida, numa primeira aproximação, como um "[...] processo matemático de conversão de mensagens, informações ou dados em um formulário ilegível por qualquer pessoa, exceto o destinatário pretendido" (Onu, 2015, p. 4), o qual protege a confidencialidade, a integridade e a autenticidade[9] do conteúdo contra acesso ou manipulação de terceiros.

Em aplicativos de mensageria privada, como WhatsApp, Telegram, iMessage, Signal, entre outros, a proteção da privacidade e segurança é anunciada (pelos provedores) como sendo a principal preocupação, eis que um dos objetivos principais das aplicações é a constituição de um meio de comunicação idôneo e seguro para a comunicação entre seus usuários, via conexão com a internet. Por meio da estrutura técnica (arquitetura) (Liguori, 2022) das aplicações, o conteúdo das comunicações fica fora do alcance de terceiros (atacantes ou adversários), sejam eles particulares, instituições privadas ou públicas, ou mesmo os Estados nacionais (Aranha, 2020). É nesse contexto em que a criptografia e todas as complexas e intrincadas questões técnico-jurídicas dela decorrentes se inserem, haja vista se tratar de uma das principais tecnologias destinadas a assegurar a confidencialidade e integridade dos dados que trafegam entre terminais de usuários dos aplicativos.

Noutro giro, não deve passar despercebido que a implementação de criptografia forte como padrão em aplicações de mensageria teve também o efeito de conferir credibilidade ao discurso dos provedores de aplicação de que os sistemas em uso, os dados que nele repousam e os que por ele trafegam não serão devassados, sequer por ordens judiciais ou emanadas por autoridades estatais. Evidentemente, a crença na indevassabilidade expande não só o número de usuários como acaba por incentivar novos usos das aplicações, permitindo o incremento do lucro de seus desenvolvedores.

A assimilação da criptografia forte, aliada à popularização do uso de aplicativos de troca de mensagens instantâneas, impactou a persecução penal e as medidas de investigação e produção probatória. A redução do fluxo de comunicação por telefone e a ampliação da comunicação digital, via internet e com criptografia, resultaram num efeito colateral de

[9] A confidencialidade garante que o acesso ao conteúdo da mensagem fique restrito às partes autorizadas. A integridade garante que a mensagem não seja modificada sem autorização. Já a autenticidade permite identificar com segurança a origem da informação. A criptografia garante, ainda, o não repúdio, prevenindo que alguém negue o envio ou recebimento de uma mensagem (ALIMONTI, 2020, p. 60).

exclusão dos órgãos envolvidos na persecução penal do acesso ao fluxo das comunicações interpessoais. As interceptações telefônicas deixaram de ser exitosas e é improvável que voltem a sê-lo, situação essa sensível para investigadores do mundo todo. Nesse sentido, Diffie e Landau retratam bem as percepções das autoridades diante da nova realidade imposta (Diffe; Landau, 2007, p. 7):

> A disponibilidade de escutas — legais ou não — por mais de uma vida nos deu gerações de policiais que não podem imaginar um mundo sem elas. Confrontados com a sugestão de perder essa ferramenta, eles respondem do mesmo modo que seria de esperar um médico moderno confrontado com a perspectiva de retornar a um mundo sem ressonância magnética, tomografia computadorizada, painéis sanguíneos e os inúmeros outros testes diagnósticos que caracterizam a medicina moderna (tradução livre).

O contínuo avanço do processo de digitalização de produtos e serviços e a elevação da permanência dos indivíduos em ambiente virtual ampliaram as fronteiras da criminalidade, o que se deu de forma ainda mais acentuada com a pandemia de Covid-19 e a necessidade de isolamento. Fraudes, crimes patrimoniais e novas formas de criminalidade se alavancaram de forma nunca vista. O foco dos órgãos estatais de investigação também vem se modificando, como se verá ao longo deste trabalho.

Com Olavo Evangelista Pezzotti, pode-se afirmar que a existência de estruturas comunicacionais eficientes é essencial ao planejamento e sucesso de ações criminosas organizadas e, justamente por isso, também interessam aos órgãos de investigação e ao Estado-juiz (senão a todos os sujeitos do processo, quando a pretensão já estiver deduzida em ação penal em curso). A correlação entre investigação de grupos ilícitos e recentes transformações nos meios de comunicação é bem retratada por Pezzotti (2022, p. 237):

> O sucesso das atividades desenvolvidas por organizações criminosas pressupõe fortes conexões entre seus membros. Sem sólida associação, grupos ilícitos operam sem sinergia e seus objetivos fracassam. E na construção de laços entre indivíduos que se unem em busca de objetivos comuns – ainda que ilegais – há um fator indispensável: a comunicação. Não existe associação entre seres humanos sem comunicação, e sem planejamento coletivo não é possível projetar ações criminosas organizadas. Somente por meio de estruturas comunicacionais eficientes, promovem-se as divisões de tarefas e estruturam-se os planos de ação das organizações criminosas. Por isso, para que os órgãos de persecução penal tenham êxito nas investigações relacionadas a tais grupos ilícitos, o emprego de técnicas de acesso às comunicações dos investigados é fundamental. Até meados da segunda década do século XXI, para o alcance desse objetivo, preponderavam, nas investigações criminais e nas atividades de inteligência de Estado, as medidas de interceptação telefônica. [...] Os smartphones trouxeram aplicações que permitem comunicações instantâneas a baixo custo, além de uma importante tecnologia para a preservação da segurança do usuário – a “criptografia de ponta-a-ponta”.

Naturalmente, irromperam reações dos órgãos estatais de segurança pública e persecução penal ao redor do mundo, dando início ao debate costumeiramente denominado como going dark (Comey, 2014). Embora não seja seu criador, a expressão foi popularizada por James Comey, ex-Diretor do FBI (Federal Bureau of Investigation, em português, Departamento Federal de Investigação dos EUA), em seus discursos entre os anos de 2014 e 2015, sendo utilizada para sintetizar os obstáculos gerados pela expansão da criptografia forte às autoridades de investigação, deixadas "na escuridão", distantes das comunicações. Como se verá, a metáfora da "escuridão" corresponde ao primeiro capítulo da fase contemporânea da já conhecida guerra criptográfica (muito presente nos anos 90 do século passado[10]), agora denominada cryptowar 2.0.

A preocupação manifestada por Comey e compartilhada pelas autoridades de investigação de todo o mundo se refere ao uso da criptografia forte como medida antiforense, isso é, como forma de destruição e ocultação ou na manipulação da fonte de prova, de forma a inviabilizar o acesso ao seu conteúdo, frustrando sua utilidade na análise forense (Costa, 2019). A propósito das implicações da criptografia como medida antiforense, veja-se (Liguori, 2022, p. 102-103):

> Medidas antiforenses são excepcionalmente problemáticas para autoridades de investigação no contexto das provas digitais, uma vez que arquivos de computador (textos, imagens, sons e vídeos) são facilmente manipuláveis, podendo ser destruídos, alterados, corrompidos ou ocultados. Uma sociedade cada vez mais digitalizada implica que a investigação criminal dependa de fontes de prova nesse âmbito. Ao inviabilizar o acesso de terceiros a conteúdos digitais, a criptografia pode ser utilizada como mecanismo de ocultação de informações de relevância para as autoridades. Mais especificamente, é possível apontar seu papel prejudicial em dois dos principais meios de obtenção de prova existentes: na busca e apreensão de dispositivos eletrônicos e na interceptação telemática (ou de dados). A criptografia de dados armazenados, aplicada ao disco rígido de computadores, celulares e outros dispositivos eletrônicos, compromete as atividades periciais em aparelhos apreendidos no âmbito de buscas e apreensões. Sob a perspectiva analógica, a busca e apreensão de coisa visa procurar e coletar objetos que podem interessar à investigação criminal (e.g., cartas e diários); tratando-se de arquivos digitais, no entanto, não basta apenas a apreensão do dispositivo eletrônico pelas autoridades, é necessário também que elas sejam capazes de acessar seu conteúdo digital. A criptografia de dados armazenados inviabiliza esse segundo passo. Por sua vez, a

[10] As guerras criptográficas tiveram sua origem na década 1990 e foram desencadeadas a partir da união de dois fatores determinantes: o lançamento da internet comercial e a disseminação dos computadores privados. O período foi marcado pela elaboração de propostas regulatórias da comunicação digital e da criptografia, compreendidas como potenciais ameaças aos poderes investigatórios dos Estados. As movimentações regulatórias ganharam projeção internacional e suscitaram reações de defensores da privacidade, de segmentos técnicos e de especialistas representantes da indústria. Nessa primeira fase, as iniciativas regulatórias acabaram sendo abandonadas ao final dos anos 1990.

> criptografia de dados em trânsito impossibilita a condução das atividades de interceptação (grifo nosso).

Após as declarações de Comey, acadêmicos, estudiosos, profissionais e desenvolvedores da criptografia (alguns deles participantes das primeiras cryptowars) se reuniram e, ainda em 2015, publicaram um relatório chamado "Keys Under Doormats: Mandating insecurity by requiring government access to all data and communications" ou, em tradução livre, "Chaves embaixo do tapete: exigências de acesso a todos os dados e comunicações pelo governo geram insegurança". A críticas se voltaram aos riscos resultantes da imposição jurídica de alternativas técnicas ao acesso excepcional, que inevitavelmente atingiram a privacidade, e consequentemente a segurança, de uma infinidade de usuários de serviços que utilizam criptografia ao redor do mundo. Salientaram, outrossim, que a continuidade do desenvolvimento de novas tecnologias, muito mais do que se limitar à elaboração de complexos sistemas criptográficos, proporcionou diversos impactos positivos para a sociedade, além de permitir novas formas de investigação e vigilância a serem manejadas sem qualquer impacto na segurança dos usuários de serviços com criptografia (Abelson, 2018)[11]. Com as novas ferramentas tecnológicas, seria equivocado pensar em "trevas" em termos de possibilidades investigatórias ou de vigilância, sendo mais adequado falar que vivemos a "era de ouro da vigilância", mesmo com a expansão da criptografia forte como padrão.

[11] Vale a transcrição de excerto do relatório que bem sintetiza as preocupações da comunidade técnica em geral: "Há vinte anos, os órgãos que fiscalizam a execução e aplicação da lei exerceram pressão política a fim de exigir que os serviços de comunicação e de dados desenvolvessem seus produtos de forma a garantir que tais órgãos obtivessem acesso a todos os dados. Após um longo debate e intensas previsões de que os canais de aplicação da lei 'ficariam limitados', essas tentativas de regulamentar a Internet emergente foram abandonadas. Nos anos que se seguiram, a inovação na Internet prosperou, e esses órgãos encontraram meios novos e mais eficazes de acessar quantidades muito maiores de dados. Hoje, estamos novamente sendo solicitados a promover normas voltadas ao fornecimento de mecanismos de acesso excepcional. Neste relatório, um grupo de cientistas da computação e especialistas em segurança, muitos dos quais participaram de um estudo em 1997 sobre esses mesmos temas, se reuniram para explorar os prováveis efeitos da imposição de mandatos de acesso extraordinários. Constatamos que o dano que poderia ser causado pelos requisitos de acesso excepcional feitos por órgãos fiscalizadores seria ainda mais intenso hoje do que há 20 anos. Considerando o crescente custo econômico e social da insegurança básica do atual ambiente da Internet, qualquer proposta que altere a dinâmica de segurança online deve ser abordada com cautela. Um acesso excepcional forçaria os desenvolvedores de sistemas de Internet a reverterem as práticas de forward secrecy que procuram minimizar o impacto na privacidade do usuário quando os sistemas são violados. A complexidade do ambiente atual da Internet, com milhões de aplicativos e serviços conectados globalmente, significa que os novos requisitos propostos por órgãos de aplicação da lei provavelmente introduzirão falhas de segurança imprevistas e difíceis de detectar. Além dessas e outras vulnerabilidades técnicas, a perspectiva de sistemas de acesso excepcional implantados globalmente gera questões difíceis sobre como tal ambiente seria governado e como garantir que tais sistemas respeitariam os direitos humanos e o Estado de direito" (Abelson et al., 2018, p. 24-26). (Liguori, 2022, p. 224). No mesmo sentido: Aranha, 2018.

O debate esteve e está presente em muitos países. O Primeiro-Ministro do Reino Unido, David Cameron, chegou a propor o banimento completo (Price, 2015) da criptografia ponta a ponta depois dos ataques de 2015 à revista Charlie Hebdo, em Paris, rogando por mais poderes às autoridades de investigação (The Guardian, 2015). Os ataques terroristas na França fizeram o debate florescer naquele país. Governos, como os da Arábia Saudita, da Rússia e dos Emirados Árabes, logo lançaram mão de legislações obrigando a retenção de dados e a desencriptação por parte de empresas de tecnologia (Berkman Klein Center, 2016).

Muito embora o escopo principal deste trabalho se volte ao exame das expectativas constitucionais de contribuir com a segurança pública/justiça que recaem sobre os provedores de aplicação de mensageria no âmbito das investigações e processos judiciais, o fato é que tal análise não pode se afastar dos temas de tecnologia que lhe são afetos, sob pena de perder de vista as bases sobre as quais repousam algumas soluções do nosso problema central.

É indispensável a compreensão de alguns termos técnicos, bem como o amplo contexto em que se insere o debate going dark e as cryptowars, o que será levado a efeito dentro dos limites pertinentes ao presente trabalho, longe de qualquer pretensão de esgotamento do tema, que é vasto e atual.

## 1.5 CRIPTOGRAFIA SIMÉTRICA, ASSIMÉTRICA E PONTA A PONTA: CONCEITOS ESSENCIAIS E UTILIDADE

Diego Aranha (2018, p. 1) observa que a preocupação com segurança da comunicação privada na presença de adversários remonta há tempos longínquos, havendo diversos registros históricos de como técnicas criptográficas foram empregadas para obter sigilo, a exemplo da Cifra de César, utilizada pelo Império Romano para estratégia militar. E prossegue o autor em sua síntese histórica:

> A tendência de utilização de criptografia pelo Estado para fins militares foi dominante durante a Idade Média, quando surgiram as primeiras unidades dedicadas a quebrar cifras utilizadas por reinos vizinhos, posteriormente ganhando enorme importância durante as Grandes Guerras. Até esse ponto, as técnicas criptográficas conhecidas sempre exigiam o compartilhamento prévio de um segredo (chave criptográfica) para comunicação confidencial, por isso chamadas simétricas. Após a disseminação de computadores e o advento de novas ideias nos anos 1970, técnicas criptográficas terminaram por se tornar de domínio civil, passando a fundamentar setores inteiros da economia, como comércio eletrônico e gerência de documentos digitais (Aranha, 2018, p. 1).

A partir do seu sentido etimológico, criptografia significa "escrita secreta", reproduzindo a clássica e ainda atual preocupação com a confidencialidade da informação. Enquanto área do conhecimento, a criptografia é o ramo que se dedica a estudo, projeto e implementação de técnicas para comunicação segura entre múltiplas partes na presença de atacantes ou adversários que tenham por objetivo impedir que as partes se comuniquem com segurança. Para atingir seu desiderato, empresas intrusivas, fraudadores ou mesmo governos autoritários devem, pois, empregar uma série de recursos e abordagens tecnológicas em suas investidas (Doneda; Machado, 2019, p. 27) .

As técnicas criptográficas estão presentes em diversos segmentos de nossas vidas, desde a navegação em sítios eletrônicos na internet, até a efetivação de transações bancárias via tablets e smartphones, e objetivam assegurar ao usuário o domínio da "exclusividade" de certas informações. Mas não são apenas as interações travadas durante a navegação na internet que são protegidas pela criptografia; também a segurança de informações e os dados armazenados em dispositivos eletrônicos são por ela assegurados contra o acesso indevido por terceiros, como nos casos de perda ou subtração do celular, por exemplo.

Nesse contexto, a criptografia consiste em técnica que permite a ocultação do conteúdo das conversas e relações desenvolvidas por meio de mecanismos eletrônicos. Como bem observa Liguori (2022, p. 43-44):

> Como técnica, a criptografia consiste na aplicação de algoritmos criptográficos (cifras) que transformam uma mensagem compreensível (plaintext) em uma mensagem cifrada (ciphertext) utilizando uma informação secreta (chave criptográfica). Somente aqueles que possuem essa informação secreta, que orienta a tradução do texto para a forma legível, conseguem compreendê-la.

A criptografia simétrica (ou criptografia de chave privada) é a forma mais simples de criptografia, eis que, nesse sistema, a mesma chave criptográfica é utilizada tanto para cifrar como para decifrar um determinado conteúdo. Quando se pensa em dados armazenados, essa modalidade de criptografia se revela particularmente útil, pois somente o usuário do dispositivo eletrônico saberá qual é a chave criptográfica (senha do smartphone, por exemplo) [12] . Todavia, o sistema simétrico ostenta graves problemas para proteção das

[12] No ponto, são ilustrativas as lições de Liguori (2022, p. 49-50): “Nos sistemas mais modernos, como smartphones com iOS, por exemplo, sempre que o dispositivo estiver bloqueado os dados armazenados estarão cifrados (iOS utiliza full disk encryption). A chave para decifrar o conteúdo é acessada uma vez que o usuário

comunicações entre ausentes, especialmente quando o cyberespaço é um meio ambiente sabidamente inseguro. Basta que se pense que, numa determinada comunicação, o emitente e o destinatário utilizarão a mesma chave para cifrar (utilizando-se de algoritmo de encriptação) e decifrar (por intermédio do algoritmo de decriptação) o conteúdo das mensagens trocadas (STALLINGS, 2015. p. 21)[13]. Caso a chave seja revelada, por qualquer motivo, a um terceiro, ele terá o poder de, a um só tempo, obter o conteúdo das mensagens (em tempo real) e se passar por um dos interlocutores da comunicação, enviando mensagens cifradas.

Para resolver essas questões, foi desenvolvida a criptografia assimétrica, também denominada de criptografia de chave pública. Esse sistema soluciona o problema utilizando um par de chaves criptográficas criadas com uma especial relação matemática entre si. Esse modelo conta com a presença de uma chave pública, livremente disponibilizada (sem nenhuma necessidade de segredo) para todos os usuários de um sistema, e uma chave privada secreta, detida por cada um dos usuários de maneira individualizada. Pela chave pública, o conteúdo da comunicação é cifrado e ocultado e, com o uso da chave privada, é decifrado e revelado, sendo também possível o fluxo inverso (Teixeira; Sabo; Sabo, 2017, p. 71).

Apesar de esses modelos serem aptos a conferir proteção aos dados, ambos contam com a possibilidade de devassa do conteúdo criptografado caso a chave criptográfica seja descoberta, o que se mostra improvável quando utilizado o modelo denominado criptografia de ponta a ponta.

A criptografia ponta a ponta (também chamado "ponto a ponto" ou "fim a fim") representa hoje uma das principais tecnologias para a garantia da segurança da informação de dados em

---

fornece uma senha ou PIN específico (a senha ou PIN não são a chave criptográfica, mas sim uma forma user-friendly de autenticar e validar o acesso a ela). Empresas como a Apple incluem esse tipo de criptografia de dados por padrão em seus sistemas operacionais – ou seja, a função já está ativada de fábrica, sem que seja necessária nenhuma configuração extra pelo usuário".

[13] William Starlins esclarece o significado de outros termos relacionados ao assunto em exame: "Uma mensagem original e conhecida como texto claro (ou plaintext), enquanto a mensagem codificada e chamada de texto cifrado (ou ciphertext). O processo de converter um texto claro em um texto cifrado e conhecido como cifração ou encriptação; restaurar o texto claro a partir do texto cifrado e decifração ou decriptação. Os muitos esquemas utilizados para a encriptação constituem a área de estudo conhecida como criptografia. Esse esquema é designado sistema criptográfico ou cifra. As técnicas empregadas para decifrar uma mensagem sem qualquer conhecimento dos detalhes de encriptação estão na área da criptoanálise, que é o que os leigos chamam de 'quebrar o código'. As áreas da criptografia e criptoanálise, juntas, são chamadas de criptologia" (Stallings, 2015, p. 21, grifos do autor).

trânsito[14], mormente em aplicativos de mensageria instantânea. O cerne do sistema consiste em cifrar, ainda no dispositivo eletrônico remetente, o conteúdo das mensagens mediante o uso de uma chave pública do destinatário. Uma vez cifrada a mensagem com a chave pública do receptor, ela só pode ser decifrada no dispositivo do receptor a partir de sua chave privada. O dado em trânsito permanece criptografado do início ao fim da comunicação, sem qualquer chance de revelação do conteúdo no caminho, de modo que nem mesmo o provedor da aplicação terá meios de acessar as mensagens que trafegam pelo sistema. Com esse expediente, a confidencialidade, a integridade e a autenticidade das mensagens trocadas são garantidas de modo que terceiros não possam lê-las ou alterá-las. Nas palavras de Aranha (2018, p. 5-6):

> Calcular e armazenar chaves criptográficas apenas nas pontas da comunicação simplifica uma aplicação criptográfica porque torna evidente quais são os principais pontos que exigem proteção, reduzindo a ameaça de pontos intermediários ou atacantes internos que operam o serviço e desfrutam de acesso privilegiado. Apesar de a designação ter se tornado comum no mercado para aplicativos de troca segura de mensagens (WhatsApp, Signal, Wire etc.), a maioria dos protocolos criptográficos modernos pode ser classificada como fim a fim. Para citar um exemplo rápido: o protocolo SSL/TLS que responde pelo acesso seguro a páginas na internet, representado pelo popular cadeado fechado em navegadores, tem como objetivo estabelecer uma conexão segura entre cliente e servidor sem a possibilidade de intervenção por pontos intermediários. Nesse sentido, aplicações de criptografia fim a fim sustentam a segurança mínima de que sistemas computacionais necessitam para realizar suas tarefas.

Nesse sistema, cada mensagem transmitida ou recebida é detentora de uma chave própria, normalmente de 128 ou 256 bits[15], sendo necessário decifrá-la para que se possa ter acesso a seu conteúdo por intermédio de interceptação (Teixeira; Sabo, 2017, p. 618-619), contudo,

[14] Sobre a diferença entre dados em trânsito, armazenados e em uso, ver: ONU, 2015; Doneda; Machado, 2019, p. 82.

[15] O Whatsapp e o Signal, utilizam o protocolo signal de chaves de 256 bits, por exemplo. Sobre a segurança do protocolo signal, os técnicos e especialistas são uníssonos em reiterar sua ausência de falhas aparentes. Anderson Nascimento, professor da Universidade de Washington, Tacoma, assevera que: "[...] depois de estudado, por diversos grupos ao redor do mundo, o entendimento da comunidade científica de criptografia é que o Signal, como se encontra hoje, o protocolo em si, é seguro. [...] o entendimento da comunidade, no momento, é que não existe uma vulnerabilidade aparente no protocolo. Então não podemos quebrar a criptografia forte". Da mesma maneira, Marcos Simplício, professor de ciência da computação da USP já afirmou que: "[…] a comunidade científica fez várias auditorias do WhatsApp, em si, e do protocolo signal. Então, é consenso na comunidade que, dificilmente, seria fácil trocar o protocolo que está sendo executado ali – logo, existe, sim, uma certa auditoria do próprio protocolo, pelo menos até onde se sabe –, e que não tem nenhuma porta dos fundos já no aplicativo. Não foi inserido jamais algo dessa natureza, também conforme as várias analises que foram feitas por pessoas independentes da comunidade científica". (Brasil. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade 5.527. Marco Civil da internet. Relatora: Ministra Rosa Weber. Arguição de Descumprimento de Preceito Fundamental. Bloqueio judicial do whatsapp. Relator: Ministro Edson Fachin. Transcrição da audiência pública. p. 48-50 Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/Alem-de-multa-empresas-de-tecnologia-que-nao-fornecem-dados-a-Justica-podem-ter-valores-bloqueados-e-nomeinscrito-em-divi.aspx. Acesso em: 2 jan. 2023.

devido à quantidade de bits envolvidos, mesmo um excelente computador levaria anos para conseguir decifrar uma única mensagem[16] que seja, o que torna inviável, para não dizer impossível, a realização de uma interceptação frutífera, seja ela lícita ou ilícita.
No mesmo sentido (Aranha, 2018, p. 104):

> Por sua vez, a criptografia de dados em trânsito impossibilita a condução das atividades de interceptação telemática: a criptografia ponta a ponta impossibilita que as autoridades acessem os conteúdos de determinada comunicação na forma legível (plaintext), mesmo que estes tenham sido interceptados com sucesso.

O modelo de criptografia de ponta a ponta pode, ainda, ser complementado por outros recursos[17], a exemplo do forward secrecy. Com o emprego desta técnica, almeja-se mitigar os danos advindos de eventuais vazamentos futuros de senhas ou chaves criptográficas que possam comprometer o conteúdo de mensagens cifradas e assinaturas digitais do passado. Uma vez implementado, o recurso fará com que para cada sessão seja criada uma chave criptográfica, a qual será descartada ao seu término[18]. No WhatsApp, por exemplo, para cada mensagem enviada ou recebida há apenas uma única chave para decifrar o seu conteúdo.

---

[16] Sendo ainda mais específico: quanto mais longa for a chave criptográfica, maior será a segurança do sistema. Assim, caso uma determinada chave criptográfica possua 128 bits, isso significa que existem $2^{128}$ possíveis combinações que um eventual invasor poderá estar sujeito a testar para revelação do conteúdo. Para quebrar uma chave de 128 bits são 340.282.366.920.938,463.463.374.607.431.768.211.456 combinações possíveis, de modo que mesmo um computador incrivelmente poderoso, com capacidade de calcular trilhões de combinações por segundo, precisaria de acabaria demorando dezenas de milhões de anos para revelar uma chave de 128 bits. Caso a chave criptográfica seja de 256 bits, aquele que desejar acesso ao conteúdo, estará sujeito a testar $2^{256}$ combinações de chaves, o que demoraria uma quantidade de tempo inimaginável. (O que é um ataque de força bruta? ataques de força bruta quebram a segurança dos dados ao tentar todas as combinações possíveis, como um ladrão que invade um cofre testando todos os números para abrir a fechadura. Disponível em: https://www.cloudflare.com/pt-br/learning/bots/brute-force-attack/. Acesso em: 03 jan. 2023.) Por outro lado, a computação quântica e a criptografia quântica prometem ser a próxima parada na evolução tecnológica e já começam a receber cada vez mais atenção por seu potencial de alteração do cenário atual. (O que é criptografia pós-quântica? A corrida para criar novas formas de proteger os dados e as comunicações da ameaça representada por computadores quânticos superpoderosos já começou. 2020. Disponível em: https://mittechreview.com.br/o-que-e-criptografiapos-quantica/. Acesso em: 02 jan. 2023.) (O que é um computador quântico?Como funciona, por que é tão poderoso e onde, a princípio, é provável que seja mais útil. 2020. Disponível em: https://mittechreview.com.br/o-que-e-um-computador-quantico/ Acesso em 02 jan. 2023.) (Aranha, 2018, p. 35).

[17] McClure e outros identificam na diversificação uma das principais estratégias para incrementar a segurança da informação: "Um dos principais mecanismos para mitigar risco é a diversificação. O que vale para investimento financeiro também funciona para a segurança da informação: com a construção de vários obstáculos diversificados, o invasor precisa investir mais e utilizar diferentes técnicas em cada ponto, aumentando o custo global de um ataque bem-sucedido mais significativamente do que com uma ou muitas contramedidas do mesmo tipo" (Mcclure; Scambray; Kurtz, 2014. p. 675).

[18] "Com o forward secrecy, uma nova chave é negociada a cada transação e as chaves de longo prazo são usadas somente para autenticação. Essas chaves de transação (ou sessão) são descartadas após cada transação – o que reduz significativamente a exposição de uma entidade que tenha sido comprometida. Quando um sistema com forward secrecy é usado, invasores que infringem uma rede e obtêm acesso às chaves só conseguirão desencriptar dados a partir do momento da violação até que esta seja descoberta e corrigida; os dados históricos permanecem seguros. Além disso, como as chaves de sessão são destruídas imediatamente após a conclusão de

Firmada a premissa pela inviabilidade técnica de revelação do conteúdo de mensagens submetidas à criptografia ponta a ponta, tem-se que eventuais alternativas técnicas para viabilizar a interceptação telemática para fins de investigação criminal passariam, necessariamente, pela diminuição das proteções geradas pela criptografia, com a criação de falhas intencionais de segurança que possibilitassem o acesso excepcional às mensagens, um dos pontos centrais do debate going dark e das propostas regulatórias da criptografia apresentadas por autoridades de investigação.

Do ponto de vista técnico, a inclusão dessas vulnerabilidades pode se manifestar de múltiplas formas, desde exigir que partes comunicantes forneçam cópia de suas chaves para as autoridades, até forçar os operadores do serviço a montar ataques de espelhamento contra seus próprios usuários (Doneda; Machado, 2019, p. 37). Os meios de acesso excepcional, também denominados backdoor, referem-se, em suma, a "[...] mecanismos ocultos, em software, em hardware ou via código malicioso, por meio do qual se acessa dispositivo ou sistema de comunicação" (Alimonti, 2020, p. 60).

## 1.6 GUERRAS CRIPTOGRÁFICAS E DEBATE GOING DARK NO BRASIL E NO MUNDO

A criptografia está presente há tempos nas comunicações digitais, todavia era restrita a públicos específicos que possuíam o conhecimento técnico para sua implementação. Tal panorama se alterou rapidamente com as revelações de Eduard Snowden (Macaskill, 2013), conforme já citado, o qual publicou uma série de documentos que davam conta que o Departamento de Defesa dos EUA detinha acesso, para fins de inteligência, a informações pessoais em massa de usuários de serviços das mais famosas companhias tecnológicas. O escândalo está na raiz do debate going dark no Brasil e no mundo e serviu de estímulo para uma forte demanda por privacidade nas comunicações on-line, transformando a proteção de dados do usuário em um grande ativo de mercado, o que modificou todo o ambiente tecnológico (Razera, 2021). A criptografia se expandiu e se popularizou, terminando por atrair a atenção de autoridades investigativas ante as proteções que proporcionava a importantes bases de dados privadas contendo informações de interesse.

---

cada transação, o invasor deve inserir-se no processo de cada transação em tempo real para conseguir obter as chaves e comprometer os dados" (Abelson *et al*., 2018, p. 17).

Após um tiroteio em San Bernardino que matou 14 pessoas e feriu outras 21 em dezembro de 2015 (Botelho; Almasy, 2015), a Justiça americana determinou que a Apple colaborasse com o FBI na reunião de informações contidas no iPhone de um dos atiradores envolvidos. O aparelho estava bloqueado por senha, e a colaboração consistia, em suma, na prestação de auxílio técnico ao FBI para superar o bloqueio (a proteção criptográfica seria desativada).[19] Ao argumento de que indigitado auxílio vulneraria o sistema de proteção com implicações de segurança graves, a Apple se negou a colaborar com a superação da barreira tecnológica. Poucos dias depois, o FBI anunciou ter obtido êxito no desbloqueio, mediante auxílio de terceiros (sem declinar quem seriam ou a técnica utilizada) e desistiu do pedido judicial.

Em um caso de tráfico de drogas e armas no Brooklyn (Nova Iorque), em fevereiro de 2016, a justiça estadunidense decidiu que a Apple entregasse à polícia o teor de mensagens trocadas via iMessage, o que foi negado pela empresa, que esclareceu ter acesso apenas ao texto criptografado das conversas. Esse caso, inclusive, acabou por servir de estímulo ao WhatsApp e aos demais aplicativos de troca de mensagens para desenvolverem seus sistemas de criptografia rumo ao método ponto a ponto.[20]

Quatro anos depois do massacre de San Bernardino, um atirador matou três pessoas em Pensacola (Flórida, EUA) em dezembro de 2019, e o FBI, novamente, agora com o apoio de William Barr (então Procurador-Geral dos Estados Unidos), buscou judicialmente o auxílio da Apple para desbloquear dois iPhones em busca de pistas[21]. Uma vez mais, o auxílio tecnológico foi negado e, por conta da pressão sobre a companhia, foi emitida uma nota pela

[19] FBI não dirá à Apple como conseguiu desbloquear iPhone de atirador: polícia federal dos eua recorreu a hackers após apple se negar a ajudar. FBIconseguiu acesso a celular de atirador que matou 14 na Califórnia. Polícia federal dos EUA recorreu a hackers após Apple se negar a ajudar. FBI conseguiu acesso a celular de atirador que matou 14 na Califórnia. 2016. Disponível em: https://g1.globo.com/tecnologia/noticia/2016/04/fbi-nao-dira-apple-como-conseguiu-desbloqueariphone-de-atirador.html. Acesso em: 06 out. 2022.

[20] Facebook, Google e WhatsApp planejam aumentar criptografia de dados de usuários: estimulados pelas batalhas da Apple contra o FBI, alguns dos maiores nomes da tecnologia estão expandindo a criptografia de dados do usuário em seus serviços, o Guardian pode revelar. Estimulados pelas batalhas da Apple contra o FBI, alguns dos maiores nomes da tecnologia estão expandindo a criptografia de dados do usuário em seus serviços, o Guardian pode revelar. 2017. Disponível em: https://www.theguardian.com/technology/2016/mar/14/facebook-google-whatsapp-plan-increaseencryption-fbi-apple. Acesso em: 06 out. 2022.

[21] Apple nega pedido do governo dos EUA para desbloquear iPhones de terrorista. 2020. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/01/15/apple-nega-pedido-do-governodos-eua-de-desbloquear-iphones-de-terroristas.htm. Acesso em: 06 out. 2022.

Apple detalhando não só as medidas de colaboração com o FBI até então efetivadas, como também a razão da empresa se negar a criar uma falha intencional no seu sistema.

Não obstante o WhatsApp não ser exatamente o aplicativo com a maior proteção à privacidade, o fato é que ele centralizou o assunto no Brasil ante a posição de destaque que ocupa quando se fala em aplicativo de troca de mensagens instantâneas. Assim foi que, em abril de 2016, o WhatsApp Inc. iniciou a utilização da criptografia de ponta a ponta como padrão, contexto esse comumente designado como um dos pontos de partida do surgimento do debate going dark no mundo:

> O que potencializou todo esse cenário e deu o pontapé inicial ao debate "going dark" foi a adoção destes mecanismos de criptografia forte por padrão em produtos e serviços extremamente populares. Quando se fala em "criptografia por padrão", o que se quer dizer é que não somente a criptografia está disponível no produto/serviço em sua modalidade mais básica, como ela também está habilitada desde o primeiro uso, não havendo necessidade de qualquer alteração de configuração do sistema para sua ativação (Liguori, 2022, p. 103).

No que tange ao WhatsApp, nos anos de 2015 e 2016, três ordens de bloqueio do funcionamento do aplicativo, alicerçadas em dispositivos do Marco Civil da Internet (especialmente em seus artigos 10 e 12)[22], foram expedidas por órgãos da jurisdição penal brasileira para compelir a empresa de tecnologia a fornecer o conteúdo de conversas a fim de instruir investigações de crimes, como organizações criminosas e tráfico interestadual de drogas. De acordo com Liguori e Salvador (2018), o WhatsApp apresentou duas justificativas centrais para motivar a impossibilidade de fornecer o conteúdo das conversas:

[22] "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. § 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. § 2º 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. [...] Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa: I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção; III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11. Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o caput sua filial, sucursal, escritório ou estabelecimento situado no País" (Brasil, 2014, grifo nosso).

> (1) de um lado, a empresa não armazena o conteúdo das conversas de seus usuários, e não haveria dispositivo legal que a obrigue a isto; (2) de outro lado, a partir de abril de 2016, o aplicativo passou a utilizar criptografia de ponta a ponta em seus serviços; como já mencionado, isso significa que somente o emissor e o destinatário conseguem acessar o conteúdo em plaintext, sendo tecnicamente impossível, dentro desse sistema, que o aplicativo tenha acesso a esses conteúdos.

A despeito da aplicação das sanções contidas no artigo 12 do MCI, as ordens judiciais que ensejaram os bloqueios foram lastreadas diretamente na técnica especial de investigação de interceptação telemática, prevista no parágrafo único do artigo 1º da Lei 9.296/1996, norma infraconstitucional de regência da matéria, que dispõe: "O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática" (Brasil, 1996). A norma em comento corresponde à regulamentação legal da parte final do inciso XII do artigo 5° da Constituição.

Após a decretação do segundo bloqueio, foram ajuizadas duas ações no STF contestando o bloqueio do aplicativo enquanto sanção imposta pelo descumprimento das ordens judiciais. Na ADPF 403, argumenta-se que seria inconstitucional o bloqueio de aplicativo como sanção, por violar a liberdade de comunicação. Já na ADI 5.527, contesta-se a constitucionalidade dos dispositivos do Marco Civil da Internet que serviram para justificar os bloqueios, isso é, os incisos III e IV do artigo 12.

Saliente-se, todavia, que as decisões de bloqueio trataram das questões envolvendo a criptografia diretamente, inclusive acerca da necessidade de incorporação de solução técnica capaz de promover o acesso ao conteúdo criptografado pelas autoridades judiciais. O assunto esteve latente no período e até mesmo o Ministério Público Federal instaurou procedimento administrativo para "[...] apurar o cumprimento de ordens judiciais de afastamento de sigilo de dados do aplicativo de comunicação WhatsApp" (Muller, 2016).

Contudo, o palco principal do debate a respeito do acesso governamental a dados criptografados no Brasil foi a audiência pública promovida pelo Supremo Tribunal Federal nos dias 2 e 5 de junho de 2017, no bojo das duas ações de controle abstrato mencionadas. Participaram 30 expositores: acadêmicos, membros da comunidade técnica, representantes da Polícia Federal, do Ministério Público Federal, do Conselho Federal da Ordem dos Advogados do Brasil, do Comitê Gestor da Internet no Brasil, integrantes de várias entidades

civis etc. Os debates desenvolvidos na audiência pública pouco se distanciaram dos pontos discutidos nos demais países, centralizando a disputa entre, de um lado,

> [...] as autoridades de aplicação da lei pressionando por mecanismos de acesso excepcional obrigatório aos sistemas de criptografia e, de outro, técnicos e acadêmicos do setor argumentando que essa solução compromete a segurança dos sistemas criptográficos e, consequentemente, a privacidade de seus usuários (Razera, 2021, p. 150).

A partir do profícuo debate plural desencadeado pelos atores envolvidos na audiência pública, foi possível detectar com maior acuidade as reais questões em jogo nas ações constitucionais. Liguori e Salvador identificam três pontos como os principais da audiência pública: (i) a possibilidade técnica de acesso aos dados criptografados; (ii) a constitucionalidade de uma possível obrigação de alterar sistemas de segurança de forma a viabilizar o acesso das autoridades; e (iii) a proporcionalidade desse tipo de medida em face dos mecanismos alternativos de investigação (Liguori; Salvador, 2018).

Um dos editais de convocação da audiência pública (Brasil, 2016) evidenciou as reais questões que os relatores pretendiam ver solucionadas, notadamente no que diz respeito aos obstáculos técnicos para a entrega do conteúdo das comunicações travadas com o uso da criptografia ponta a ponta no WhatsApp. Nele, fez-se constar algumas perguntas que deveriam ser respondidas como requisito à participação na audiência:

> 1 – Em que consiste a criptografia ponta a ponta (end to end) utilizada por aplicativos de troca de mensagens como o WhatsApp?
> 2 – Seria possível a interceptação de conversas e mensagens realizadas por meio do aplicativo WhatsApp ainda que esteja ativada a criptografia ponta a ponta (end to end)?
> 3 – Seria possível desabilitar a criptografia ponta a ponta (end to end) de um ou mais usuários específicos para que, dessa forma, se possa operar interceptação juridicamente legítima?
> 4 – Tendo em vista que a utilização do aplicativo WhatsApp não se limita a apenas uma plataforma (aparelhos celulares/smartphones), mas permite acesso e utilização também em outros meios, como, por exemplo, computadores (no caso do WhatsApp mediante o WhatsApp Web/Desktop), ainda que a criptografia ponta a ponta (end to end) esteja habilitada, seria possível "espelhar" as conversas travas no aplicativo para outro celular/smartphone ou computador, permitindo que se implementasse ordem judicial de interceptação em face de um usuário específico?[123]

Em fevereiro de 2019, o Ministério da Justiça e Segurança Pública promoveu, em Brasília, o primeiro simpósio sobre going dark no Brasil (2019). O evento contou com a presença de representantes de 12 países e reverberou as preocupações das autoridades de persecução ante os desafios e impactos gerados em suas atividades pela assimilação das técnicas de

criptografia forte. Ao final, os participantes assinaram um documento intitulado “Declaração Going Dark Brasil” (2019), que bem resume os anseios e preocupações gerais dos que laboram no sistema de justiça penal:

> O advento da Internet e das comunicações digitais transformou a economia global e enriqueceu a sociedade civil. Nações democráticas valorizam os direitos pessoais e a privacidade e apoiam o papel das tecnologias de criptografia na proteção desses direitos nesta era digital. Nesses países, o acesso das autoridades policiais às informações de cidadãos particulares – seja em suas casas, bens pessoais ou dispositivos – é uma circunstância excepcional, que ocorre apenas em conformidade com o estado de direito e o devido processo legal.
> Infelizmente, criminosos e terroristas exploram cada vez mais esses avanços tecnológicos recentes. Dispositivos eletrônicos pessoais e aplicativos de comunicação são criados sem considerar adequadamente as consequências da segurança pública, portanto, impedem o acesso a provas fundamentais para impedir crimes graves e ameaças à segurança nacional. Isso impõe obstáculos difíceis e às vezes intransponíveis à capacidade das autoridades de segurança pública de prevenir a violência, proteger as vítimas e processar criminosos. Este tema não é apenas um problema na aplicação da lei, mas uma responsabilidade mútua para todas as partes interessadas, incluindo fornecedores de hardware, software e serviços.
> Os participantes do Simpósio Going Dark Brasil, ocorrido em Brasília, nos dias 1 1 e 12 de fevereiro de 2019. reconhecem o tema como uma preocupação internacional premente. A crescente distância entre o tempo do pedido e a autorização legal para obter provas fundamentais e os desafios tecnológicos para fazê-lo, é um problema complexo que requer atenção internacional urgente e continuada. Sem esse esforço, arriscamo-nos a uma corrosão do estado de direito que é vital para a sociedade democrática (grifos nossos).

Seguindo a toada histórica do debate, em maio de 2020, depois de quase três anos de realização da citada audiência pública, a ADPF 403 e a ADI 5.527 foram pautadas e receberam os votos dos seus respectivos relatores, os quais se posicionaram contra as ordens de bloqueio como sanção ao descumprimento das decisões judiciais, firmando a imprescindibilidade das técnicas criptográficas para a fruição de diversos direitos fundamentais. Com esse entendimento, rejeitaram a possibilidade de enfraquecimento da criptografia para fins de investigação criminal.

No bojo da ADPF 403, o Ministro Edson Fachin registrou, lastreado, dentre outros, nos trabalhos de David Kaye, Abelson e outros e Diego Aranha (ONU, 2015; Abelson et al., 2015; Aranha, 2018), a importância da criptografia para o exercício de direitos fundamentais, como a privacidade, a liberdade de expressão e a comunicação longo, porém ilustrativo, excerto:

> É contraditório, portanto, que em nome da segurança pública deixe-se de promover e buscar uma internet mais segura. Uma internet mais segura é direito de todos e dever do Estado. 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. À luz de todas essas considerações, poder-se-ia, então, questionar se a criptografia ponta a ponta poderia ser restrita apenas a agentes de governo, isto é, se seria possível proibir o acesso da criptografia a todos os cidadãos. A resposta, aqui, seria negativa. Além de promover aspectos fundamentais da vida humana como a proteção à integridade, ao sigilo, à confidencialidade, à autenticidade e à privacidade das mensagens transmitidas, a criptografia assegura um acesso mais justo a pessoas que estão em situação de vulnerabilidade. Padrões sistemáticos de vigilância e mensagens dirigidas impactam desproporcionalmente essas pessoas, seja porque têm menos acesso aos meios de proteção, seja porque barreiras impedem seu acesso a essas ferramentas em absoluta condição de igualdade. 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. (…) Por entender que o risco causado pelo uso da criptografia ainda não justifica a imposição de soluções que envolvam acesso excepcional ou ainda outras soluções que diminuam a proteção garantida por uma criptografia forte, penso que não há como obrigar que as aplicações de internet que ofereçam criptografia ponta a ponta quebrem o sigilo do conteúdo de comunicações, ao menos à luz das informações que traduzem o consenso científico atual sobre a matéria (grifos do autor) (Brasil, 2020).

Na ADI 5.527, a Ministra Rosa Weber seguiu na mesma linha do Ministro Fachin, fundamentando seu entendimento em consideração dos trabalhos de Kaye, da ONU, e de Schulz e van Hoboken[128], da Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO):

> Questiona-se, na sequência, a licitude do uso, nas comunicações privadas, de tecnologias de proteção do sigilo e da segurança das comunicações, notadamente das tecnologias criptográficas que tornem materialmente inviável o cumprimento, pela plataforma, de eventual comando judicial de disponibilização do conteúdo de comunicações privadas havidas por seu intermédio. […] Entendo que a resposta no ponto é negativa. O poder de o Estado determinar a disponibilização do conteúdo de mensagens no âmbito de investigação criminal ou da instrução processual penal não conduz à conclusão de que ilegal o oferecimento de serviço que adote tecnologia por força da qual inacessível, esse conteúdo, ao próprio provedor da plataforma. Uma vez desenvolvida e adotada por ele, um particular, tecnologia voltada a garantir a segurança e a privacidade de comunicações, e oferecida essa tecnologia, como valor agregado, a outros particulares que contratam seus serviços, 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. […] a difusão da criptografia também tem garantido a segurança da comunicação de grupos de direitos humanos e indivíduos que se mobilizam contra regimes opressivos ao redor do mundo. Em certa medida, a liberdade fundamental que assegura ao indivíduo o direito de fechar o portão de casa com um cadeado, elevar a altura do muro ou pendurar uma cortina na janela, autoriza cogitar uma espécie de direito fundamental à criptografia, ou pelo menos que o uso da criptografia consiste em uma ferramenta indispensável, nos dias de hoje, para assegurar o direito à privacidade (Brasil, 2020).

As ações ainda estão pendentes de julgamento definitivo no Supremo Tribunal Federal após pedido de vista feito pelo Ministro Alexandre de Morais.

Ainda em 2020, as cryptowars também se manifestaram no Superior Tribunal de Justiça, que, por intermédio de sua 3ª Seção (Brasil, 2020), fez coro aos argumentos ventilados por Rosa Weber e Edson Fachin, e julgou ser incabível a imposição de astreintes como medida coercitiva pelo descumprimento de decisão judicial de quebra de sigilo de dados, reconhecendo textualmente impossibilidade técnica ante o emprego de criptografia de ponta a ponta:

> Convém ressaltar que, tanto o Ministro Edson Fachin quanto a Ministra Rosa Weber, ao fim de seus votos, chegam, ambos, à mesma conclusão: o ordenamento jurídico brasileiro não autoriza, em detrimento da proteção gerada pela criptografia de ponta a ponta, em benefício da liberdade de expressão e do direito à intimidade, sejam os desenvolvedores da tecnologia multados por descumprirem ordem judicial incompatível com encriptação. [...] Por isso, embora chamando atenção para os graves aspectos que neste meu voto inicialmente levantei, curvo-me aos argumentos apresentados pelos em. Ministros Rosa Weber e Edson Fachin, os quais representam, ao menos até a presente altura, o pensamento do Supremo Tribunal Federal na matéria. E, assim, endosso a ponderação de valores realizada pelos aludidos Ministros, que, em seus votos, concluíram 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 (Brasil, 2020).

Em junho de 2021, a Quinta Turma do Superior Tribunal encampou o entendimento da 3ª Seção e firmou o descabimento da imposição de multa a provedores de mensageria em razão de descumprimento de ordem judicial por impossibilidades técnicas relacionadas à criptografia.[132] Em novembro de 2022 o STJ decidiu que empresas de internet que prestam serviços em território nacional devem se submeter à lei brasileira e manteve multa imposta como penalização pela prática de ato atentatório à dignidade da Justiça, consistente na recalcitrância injustificada ao cumprimento de decisão judicial que determinou a entrega de dados armazenados fora do território nacional (embora não por razões relacionadas à criptografia) (Brasil, 2022). Soma-se que o STJ também já decidiu que, além da multa, as empresas de tecnologia que desobedecerem a ordens de entrega de dados à Justiça estarão sujeitas ao sancionamento com o bloqueio de valores e inscrição em dívida ativa (Brasil, 2020).

Paralelamente aos debates desenvolvidos nas ações constitucionais no Supremo Tribunal Federal e demais feitos judiciais nos tribunais superiores citados, foram apresentados alguns

projetos de lei (PL) no Congresso Nacional na busca por soluções para as autoridades de persecução, dentre os quais se destacam[23] o PL

O PL 9.808, proposto pelo Deputado João Campos, objetiva inserir dois parágrafos ao art. 10[24] do Marco Civil da Internet para: (i) possibilitar à autoridade policial o acesso aos conteúdos de dispositivos móveis sem autorização judicial nas hipóteses de flagrante de crimes hediondos, tráfico de drogas e terrorismo; e (ii) em abordagem regulatória da criptografia, obrigar que os provedores de aplicações entreguem as chaves criptográficas. Logo se vê que a proposição não observa as hipóteses em que a entrega das chaves é inviável tecnicamente para o provedor da aplicação, a exemplo dos casos em que adotada a criptografia de ponta a ponta.

Já o PL 10.372, cujo autor foi o Deputado José Rocha, estabelece obrigação de fornecimento de chaves criptográficas quando existir a infiltração de agente policial. Nesse projeto de lei, o que se propõe é a previsão, no § 6º do art. 10 da Lei de Organizações Criminosas (Lei nº 12.850, de 2 de agosto de 2013), de que "[...] a infiltração incluirá a possibilidade de acesso, pela autoridade policial, a chave criptográfica de provedores de internet, provedores de conteúdo e autores de aplicativos de comunicação" (Brasil, 2018). Ainda merece menção o denominado "Pacote Anticrime", eis que previa, no texto original, a ampliação dos poderes de interceptação

Também o projeto do novo Código de Processo Penal (CPP) reverberou controvérsias, visto que seu texto preliminar contemplou, dentre outras, a previsão de obrigação de assistência dos provedores de serviços de telecomunicações, os quais teriam o dever legal de disponibilizar

[23] Para uma análise mais ampla das propostas legislativas que, de alguma forma, enfraquecem a criptografia, conferir: Ramiro, 2020.

[24] "§ 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" (Disponível em: em: https://obcrypto.org.br/wp-content/uploads/2020/08/O-mosaico-legislativo-da-criptografia-noBrasil-uma-an%C3%A1lise-de-Projetos-de-Lei-1.pdf. Acesso em: 4 ago. 2022.
de órgãos investigativos estatais e pressupunha o dever das plataformas de colaborar para com a persecução penal, sendo que deixava subentendida a extensão dessas obrigações para provedores de serviços protegidos por criptografia forte.

recursos e meios tecnológicos necessários à implementação de interceptação das comunicações (Pereira; Rodrigues, 2021).

Outra iniciativa que rendeu forte discussão foi o Projeto de Lei nº 2.630/20 (proposto pelo senador Alessandro Vieira -Cidadania-SE), que busca implantar a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet (batizado como "PL das fake news"). Por intentar criar mecanismo de monitoramento vinculado ao conteúdo de mensagens encaminhadas massivamente, o projeto poderia afetar a higidez da criptografia de ponta a ponta, com reflexos sobre a liberdade de expressão e outros direitos (Abreu; Antonialli, 2022).

Em vertente diametralmente oposta aos projetos de lei anteriormente citados, o anteprojeto para a "LGPD penal", capitaneado pelo ministro do Superior Tribunal de Justiça, Nefi Cordeiro, e inspirado sobretudo na vigente LGPD e na Diretiva 680/2016 da União Europeia, atribuiu licitude ao uso da criptografia ponta-a-ponta, desobrigando a entrega de dados por pessoas jurídicas de direito privado que não coletem ou retenham dados. (arts. 11, §3º e 42, § 3º, II[25]). O anteprojeto, no entanto, ainda não foi formalmente apresentado no Congresso Nacional.

Lado outro, importa esclarecer que, em 2016, foi sancionado o Decreto nº 8.771, de 11 de maio, que regulamenta o Marco Civil da Internet. Apesar de o decreto não trazer em seu teor instrumentos normativos de regulação da criptografia ou que instituam obrigações aos provedores de aplicação, ele termina por recomendar o uso das técnicas criptográficas como medidas de proteção por parte de provedores de conexão e de aplicações, na guarda, no armazenamento e no tratamento de dados pessoais e comunicações privadas:

> Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança:
> […]
> IV - o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes (Brasil, 2016).

[25] Art. 11. O acesso de autoridades competentes a dados pessoais controlados por pessoas jurídicas de direito privado somente ocorrerá mediante previsão legal, respeitados os princípios desta Lei. [...]

Em arremate ao tópico, cabe frisar que muito embora todos os poderes constituídos tenham tomado parte, em alguma medida, no debate sobre as criptografia e persecução penal, fica patente o protagonismo assumido pelo Poder Judiciário no encaminhamento institucional de questões que estão na ordem do dia para autoridades de persecução e que, ao fim e ao cabo, refletem em maior ou menor impunidade. Com efeito, o Poder Judiciário ocupa papel central na luta pela construção de um sistema punitivo funcional e que esteja à altura das aspirações de um Brasil democrático, comprometido com os direitos humanos e com o progresso social[143]. Nas palavras de Barrozo, "a verdade é que ao redor do mundo, o judiciário é o agente político mais promissor de reformas fundamentadas em muitas áreas de progresso social" (Barrozo, 2014. p. 6).

## 1.7 REGULAÇÃO DA CRIPTOGRAFIA NO BRASIL E OBRIGAÇÃO DE ASSISTÊNCIA DOS PROVEDORES DE APLICAÇÃO

### 1.7.1 Tratamento da criptografia no ordenamento jurídico positivo

Em que pese o ordenamento jurídico brasileiro não contemplar regulação específica da criptografia, é viável considerar que diversas normas fomentam a ampliação do seu uso.

O Marco Civil da Internet preleciona que a disciplina do uso da internet no Brasil segue alguns princípios, dentre os quais se destaca a necessidade de preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas
(art. 3º, inciso V).

Na mesma linha, o decreto que regulamentou do Marco Civil elencou, dentre suas diretrizes de segurança, a criptografia como solução técnica destinada à gestão de registros e garantia da inviolabilidade dos dados (art. 13, IV).

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) não destoou do Marco Civil e trouxe como princípios da proteção de dados a boa fé e segurança, que, na dicção legal, consiste na "[...] utilização de medidas técnicas e administrativas aptas a proteger os dados

pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão" (Brasil, 2018).

Em seu artigo 46, a LGPD estabeleceu que aqueles que promovam o tratamento de dados devem adotar medidas de segurança, técnicas e administrativas para a proteção dos dados pessoais contra acessos não autorizados, situações acidentais ou ilícitas (seja destruição, perda, alteração ou comunicação), ou operações inadequadas.

Já o artigo 47 da norma de regência preconiza que qualquer pessoa que atue em qualquer fase do tratamento de dados fica obrigada a garantir a segurança dos dados pessoais, mesmo após o seu término do tratamento. Os artigos 48, § 3º, e 52, § 1º, VIII, da LGPD também cuidam do tema de segurança de dados:

> Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
> § 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.
> [...]
> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
> § 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:
> [...]
> VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei (Brasil, 2018).

Merece registro também a iniciativa veiculada na Lei nº 13.964, de 24 de dezembro de 2019, o denominado "Pacote Anticrime", que atribuiu ao juiz das garantias, de forma lacônica, a competência de decidir acerca dos pedidos de "[...] interceptação telefônica, do fluxo de comunicações em sistemas de informática e telemática ou de outras formas de comunicação" (Brasil, 2019).

A Lei de Acesso à Informação (LAI - Lei 12.527/2011) cuidou de estabelecer disposições acerca dos procedimentos e ações para implemento de segurança no tratamento de informações de natureza sigilosas:

> Art. 25. É dever do Estado controlar o acesso e a divulgação de informações sigilosas produzidas por seus órgãos e entidades, assegurando a sua proteção.
> § 3º Regulamento disporá sobre procedimentos e medidas a serem adotados para o tratamento de informação sigilosa, de modo a protegê-la contra perda, alteração indevida, acesso, transmissão e divulgação não autorizados.
>
> Art. 26. As autoridades públicas adotarão as providências necessárias para que o pessoal a elas subordinado hierarquicamente conheça as normas e observe as medidas e procedimentos de segurança para tratamento de informações sigilosas (Brasil, 2022).

De acordo com o decreto regulamentador (Decreto 7.845/2012) da LAI, nos sistemas informáticos em que ocorrer tratamento de informações classificadas, necessariamente deverão ser adotados recursos criptográficos adequados ao nível de sigilo, hipótese em que as operações de cifragem e decifragem deverão ser operacionalizadas com o uso de algoritmos de Estado, definidos como "função matemática utilizada na cifração e na decifração, desenvolvido pelo Estado, para uso exclusivo em interesse do serviço de órgãos ou entidades do Poder Executivo federal". O decreto ainda conceitua cifração, decifração e recurso criptográfico:

> Art. 2º Para os efeitos deste Decreto, considera-se:[...]
> II - cifração - ato de cifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para substituir sinais de linguagem clara por outros ininteligíveis por pessoas não autorizadas a conhecê-la;
> VIII - decifração - ato de decifrar mediante uso de algoritmo simétrico ou assimétrico, com recurso criptográfico, para reverter processo de cifração original;
> XVII - recurso criptográfico - sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração; e

Frise-se, por fim, que a criptografia é mencionada 9 vezes no Decreto nº 10.222/2020 (Brasil, 2020), que instituiu Estratégia Nacional de Segurança Cibernética (E-Ciber), no âmbito da administração pública federal. Dentre outras disposições, a norma prevê como ação estratégica da e-ciber:

> Promover um ambiente participativo, colaborativo e seguro, entre as organizações públicas, as instituições privadas, a academia e a sociedade, por meio do acompanhamento contínuo e proativo das ameaças e dos ataques cibernéticos, com o objetivo de [...] estimular o uso de recursos criptográficos, no âmbito da sociedade em geral, para comunicação de assuntos considerados sensíveis (Brasil, 2020).

### 1.7.2 Obrigação de assistência dos provedores de aplicação

Cabe à Agência Nacional de Telecomunicações (Anatel), por força da Lei nº 9.472, de 16 de julho de 1997 (Lei Geral de Telecomunicações), a regulação das atividades desenvolvidas

pelos provedores de telecomunicação, sendo que o órgão disciplinou as obrigações específicas de assistência às autoridades de investigação em alguns de seus atos normativos.

Conforme compilação de Abreu e Antonialli (2022, p. 49), a Resolução nº 738/2020, trouxe alterações às Resoluções 426/05 (regula o seguimento de provedores de telefonia fixa) e 477/07 (regula o seguimento de provedores de telefonia móvel), substituindo-as em matéria de sigilo, prevenção à fraudes e medidas de apoio à órgãos de segurança pública. Embora não citada por Abreu e Antonialli, também a Resolução nº 614/2013 (regula o seguimento de provedores de conexão à internet) teve seu texto modificado pela Resolução nº 738/2020.

Muito embora as alterações não tenham alterado significativamente a disciplina das obrigações de assistência por parte dos prestadores de serviços de telecomunicações, agora o regramento das obrigações de apoio à segurança pública está reunido sob a rubrica do artigo art. 65-K da Resolução nº 738/2020, que assim dispõe:

> Art. 65-K. As prestadoras devem tornar disponíveis os recursos tecnológicos, facilidades e dados necessários à suspensão de sigilo de telecomunicações, determinada por autoridade judiciária ou legalmente investida desses poderes, e manter controle permanente de todos os casos, acompanhando a efetivação dessas determinações, e zelando para que elas sejam cumpridas, dentro dos estritos limites autorizados.
> § 1º Os equipamentos e programas necessários à suspensão do sigilo devem integrar a plataforma da prestadora, que deve arcar com os respectivos custos.
> § 2º Os demais custos operacionais relacionados a cada suspensão de sigilo poderão ter caráter oneroso para a autoridade demandante.
> § 3º A Anatel deve estabelecer as condições técnicas específicas para disponibilidade e uso dos recursos tecnológicos e demais facilidades referidas neste artigo, observadas as disposições constitucionais e legais que regem a matéria.

Provedores de aplicação, contudo, não estão sujeitos à disciplina da Anatel, havendo lacuna regulatória no que tange às obrigações de assistência deles às autoridades de investigação. Logo, atualmente "[...] não há na legislação brasileira obrigação oponível aos desenvolvedores de aplicativos de mensagens no sentido de construírem interceptações" (Abreu, Antonialli, 2022, p. 37). Como alertam Jaqueline Abreu e Dennys Antonialli:

> Apesar de todo arcabouço regulatório da Anatel, essa agência não é responsável pela regulação dos principais agentes de comunicação atuais, que é o caso dos serviços de mensageria privada e os provedores de conteúdo na internet. Com isso, seus atos de vigilância possuem incidência limitada aos serviços de telecomunicação no Brasil, como a internet banda larga, a telefonia fixa ou os planos de celular, que já não são o espaço de maior relevância para a comunicação e a troca de mensagens entre os cidadãos (Abreu, Antonialli, 2022, p. 37).

Cumpre esclarecer que a obrigação de viabilizar recursos tecnológicos necessários à operacionalização da suspensão de sigilo de telecomunicações difere da obrigação de quebra de criptografia, a qual possibilitaria (por meio ataques de força bruta, obrigação de entrega de chaves ou qualquer outro meio) o acesso a todo um universo de conteúdo de comunicação pretérita criptografada, já que originalmente somente os detentores da chave da criptografia conseguem decifrar o conteúdo das mensagens. A obrigação de disponibilizar recursos tecnológicos referido na Resolução da Anatel destina-se à operacionalização da suspensão de sigilo de serviços telecomunicações sujeitos às competências da agência reguladora (empresas de telefonia e provedores de conexão) em razão de ordens judiciais de interceptação, por prazo determinado, do fluxo das comunicações (em tempo real) em sistemas informáticos e telemáticos; a obrigação de assistência está alinhada com a norma de regência, que é Lei nº 9.296, de 24 de julho de 1996 (Lei de Interceptações Telefônicas e Telemáticas), que prevê em seu artigo 7º que "para os procedimentos de interceptação de que trata esta Lei, a autoridade policial poderá requisitar serviços e técnicos especializados às concessionárias de serviço público (Brasil, 1996)".

A toda evidência, o ordenamento jurídico em vigência parece incentivar o uso da criptografia para proteção de dados e informações sigilosas em geral, inexistindo, até o momento, previsões normativas expressas no sentido de restringir o uso de criptografia por provedores de aplicações de internet ou impor a estes obrigações de fornecimento de chaves criptográficas ou criação de mecanismos tecnológicos de acesso excepcional ao conteúdo de comunicações criptografadas. Exsurge que qualquer decisão judicial que objetive impor tais obrigações deverá, necessariamente, sopesar a incidência do princípio da legalidade civil, segundo o qual "ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei" (art. 5º, II,
CF).

# 2 CRIPTOGRAFIA, PROVEDORES DE APLICAÇÃO DE MENSAGERIA E A TEORIA DOS DEVERES FUNDAMENTAIS NA ERA DIGITAL

De um modo geral, a regulação do meio ambiente digital sob as perspectivas dos deveres fundamentais é tema pouco estudado pela doutrina brasileira (Colnago, 2014), mas que se mostra profundamente apropriado à compreensão do papel dos provedores de mensageria diante de decisões judiciais que determinem a entrega de dados inertes em formato legível (seja porque não afetados pela criptografia, seja porque disponíveis as chaves criptográficas).

## 2.1 DESCUMPRIMENTO DE DECISÕES JUDICIAIS DE INTERCEPTAÇÃO TELEMÁTICA E QUEBRA DE SIGILO DE DADOS E DEVERES FUNDAMENTAIS: UM PANORAMA DE TENSÕES

A disputa entre empresas tecnológicas e autoridades de investigação produziu amplo debate sobre uso da criptografia como tecnologia de segurança da informação, atraindo manifestações de diversos segmentos da comunidade técnica, indústria, academia e diversas autoridades.

Por repercutirem com maior intensidade as causas e consequências das guerras criptográficas, viram-se nos EUA alguns dos embates mais contundentes entre os atores envolvidos.

A face contemporânea das guerras criptográficas chegou ao Brasil, e as audiências públicas alargaram as perspectivas em torno do pujante tema dos bloqueios do aplicativo WhatsApp, o mais popular do gênero entre nós. Não é demais assumir que foi a partir daí que a importância da criptografia e os desafios que ela impõe às autoridades foram projetadas para fora dos segmentos especializados.

Ao implementarem a criptografia forte como padrão, retirando o poder de acesso ao conteúdo de mensagens, e recusarem o cumprimento de ordens judiciais que determinavam formas de acesso excepcional aos conteúdos cifrados, companhias tecnológicas fizeram eclodir não só o debate sobre a regulação da criptografia em si, como também sobre a colaboração dessas companhias para com os órgãos estatais envolvidos na persecução penal, já que a popularização de produtos e serviços digitais possibilitariam novas técnicas investigativas.

Diversos relatórios, artigos e trabalhos científicos foram publicados defendendo a necessidade de higidez da criptografia, bem como apontando novas possibilidades de acesso a dados e metadados (naturalmente já conhecidas dos arquitetos das aplicações).

Ao lado dessas questões, outras se colocaram.

O Telegram esteve nos holofotes do tema "bloqueio" de aplicativos ao negar cumprimento de decisões do Supremo Tribunal Federal. Após o descumprimento de uma série de decisões judiciais, o Ministro Alexandre de Moraes decidiu, no bojo da Petição 9.935 do Distrito Federal, suspender temporariamente os serviços da aplicação, invocando, para justificar a sanção do artigo 12, inciso III, do MCI, o descumprimento do art. 10, § 1º, do mesmo diploma (Brasil, 2001).

A suspensão repercutiu em diversos meios de comunicação. A decisão revisitou o histórico de descumprimentos de decisões até aquele momento. Nos autos do Inquérito (Inq.) nº 4.781/DF, foi determinada a exclusão de publicações e o bloqueio de um determinado canal, com o fornecimento de seus respectivos dados cadastrais. Já em 2022, nos autos da Petição 9.935/DF, decidiu-se que o Telegram bloqueasse três perfis de um usuário, fornecendo dados cadastrais do criador dos perfis, além de implementar mecanismos de desmonetizarão; ante o desatendimento, a decisão foi reiterada, agora com a intimação "[…] do procurador constituído pela pessoa jurídica estrangeira, com domicílio no Brasil, com poderes para representá-la administrativa e judicialmente (art. 217 da Lei 9.279/96)" (Brasil, 2001), sob pena pagamento multa diária de R$ 100 mil por perfil não bloqueado (conforme arts. 77, IV, e 139, IV, do Código de Processo Civil, combinados com o art. 3º do Código de Processo Penal).

Uma terceira decisão foi prolatada e, finalmente, foi determinada a suspensão completa e integral do funcionamento do Telegram no Brasil até que todas as decisões anteriores fossem totalmente cumpridas, inclusive com o pagamento das astreintes e com a indicação, em juízo, da representação oficial no Brasil (pessoa física ou jurídica). Para o caso de novo descumprimento do Telegram, as astreintes foram majoradas para R$ 500 mil. Para efetivação da decisão de suspensão, a Anatel, o Google, a Apple e as empresas provedoras de serviço de internet (Oi, Sky, Live Tim, Vivo, NET Virtua, GVT) deveriam implementar as medidas necessárias para obstar o funcionamento da indigitada aplicação de mensageria. No mesmo

dia em que prolatada esta última e drástica decisão, Pavel Durov, criador e CEO do Telegram, fez contato com o Supremo Tribunal Federal e disse "[...] que um problema com e-mails impediu a plataforma de receber as ordens judiciais do STF, pediu desculpas e prometeu cooperação" (Vital, 2022).

A despeito da multicitada dificuldade de contato com representantes para cumprimento dos comandos judiciais, soube-se, posteriormente, que o Telegram matinha representante no Brasil há sete anos (Rocha, 2022).

Acresça-se que o Telegram Messenger Inc. também ignorou múltiplos pedidos de cooperação do Tribunal Superior Eleitoral (TSE) (Rocha, 2022), a evidenciar sua contumácia em descumprir, sem qualquer justificativa plausível, as decisões emanadas da Justiça Eleitoral brasileira.

Sediado em Dubai, o Telegram possui servidores em várias partes do mundo, mas não no Brasil (Franco, 2022), e já foi indisponibilizado ou teve seu funcionamento restringido em, ao menos, 11 países (Cardoso, 2022).

Diferentemente dos casos que colocaram o WhatsApp no centro dos debates na ADPF 403 e na ADI 5.527, o descumprimento pelo Telegram das decisões do STF e do TSE nada tem a ver com criptografia ou barreiras tecnológicas, muito embora também envolva o acesso a dados de usuário localizados em servidores fora do Brasil.
Trata-se, a toda evidência, de estratégia empresarial[26].

Não é de se estranhar que o cumprimento/descumprimento de decisões judiciais seja um dos elementos mais recorrentes em várias inserções do latente debate sobre os desafios da persecução penal na era da digital, que, a um só tempo, traz consigo problemas próprios da adoção de tecnologias de segurança da informação, mas também dificuldades de se obter a colaboração das empresas de tecnologia, mesmo quando ausentes obstáculos técnicos. Não

[26] Hoffmann-Riem anota que, atualmente, o próprio desenvolvimento da internet está vinculado a decisões de entidades privadas e empresariais. Recebida por muitos, em sua origem, como um espaço de desenvolvimento livre, pautado na autoconfiguração e autorregulamentação autônomas dos atores nela envolvidos, a internet se modificou substancialmente com a consolidação do oligopólio hoje verificado. Nas suas palavras: "As mudanças consideráveis – que foram exacerbadas pela oligopolização de grandes áreas – mudaram radicalmente o caráter da Internet como meio de liberdade para todos e com direitos iguais de acesso e uso para todos" (Hoffmann-Riem, 2022, p. 257-258).

bastasse, a obtenção de dados digitais ainda traz um problema adicional, diretamente ligado à sua natureza imaterial, que é o limite territorial da jurisdição estatal, já que os dados digitais armazenados podem estar alojados em qualquer parte do mundo, não sendo incomum que repousem em provedores situados fora do país onde se dá a investigação.

É desse cenário que extraímos a importância de enxergar o problema a partir da perspectiva das disputas judiciais entre provedores de aplicação e autoridades de persecução, com apoio no aporte teórico fornecido pela teoria dos deveres.

fundamentais, mormente quando se verifica certa escassez de trabalhos sob essa ótica. O recorte se assenta na necessidade de compreensão das questões que compõem conflitos entre os provedores de aplicações e o poder público em sua inteireza, o qual perpassa, inevitavelmente, pela análise das condutas dos atores envolvidos em disputas judicializadas, dada a inafastabilidade da jurisdição (art. 5º, XXXV, CF).

Tais conflitos estão na ordem do dia para todo o sistema de justiça penal brasileira, para as entidades privadas que exploram aplicações de mensageria e mesmo para os usuários de aplicativos (ainda que não tenham real consciência disso), que eventualmente podem ser afetados pelas sanções de indisponibilização de serviços. Órgãos policiais, Ministério Público e diversas instâncias judiciárias com competência criminal olham com atenção para o encaminhamento desses conflitos, mormente os que se encontram submetidos ao exame da jurisdição constitucional por força do controle abstrato e concentrado de constitucionalidade.

Repise-se que vários dos embates ocorridos na versão recente das guerras criptográficas tiveram como pano de fundo a presença de ordens judiciais destinadas à obtenção de acesso a dados digitais. WhatsApp, iMessage e Telegram são apenas exemplos de aplicações de mensageria que protagonizaram, em algum momento, tais discussões em um cenário amplo e mundial de confrontos, sendo crível que novos embates de semelhante natureza venham a ocorrer.

Hodiernamente, é impróprio considerar as telecomunicações digitais como mero instrumento de troca de comunicação. Trata-se, isso sim, de verdadeira infraestrutura básica quase onipresente, que pode, e será, utilizada para os mais diversos fins (Hoffmann-Riem, 2022, p. 69), lícitos ou ilícitos. E os aplicativos de mensageria estão entre as ferramentas digitais com

maior penetração na sociedade, estando presentes na quase totalidade dos smartphones conectados à internet. O uso do WhatsApp, por exemplo, beira à unanimidade nos celulares brasileiros, atingindo, no mês de agosto de 2022, 99% dos dispositivos eletrônicos, conforme o Panorama Mobile Time/Opinion Box sobre mensageria no Brasil. Segundo a pesquisa, o Instagram é encontrado em 82% dos aparelhos, o Facebook Messenger em 71% e o Telegram em 60% dos dispositivos móveis (Mobile Time, 2022).

É cediço que os múltiplos e massivos usos de aplicações de troca de mensagens exigem, naturalmente, o emprego de tecnologias de segurança da informação confiáveis, todavia entendemos que a proteção ofertada pelo direito não deve se voltar apenas à salvaguarda de dados individuais e pessoais, devendo contemplar também os riscos advindos da digitalização das comunicações. Nas palavras de HoffmannRiem, "[...] a visão deve ser ampliada tanto em termos sociopolíticos como jurídicos, ou seja, para incluir as oportunidades e os riscos da digitalização no Estado e na sociedade" (Hoffmann-Riem, 2022, p. 69). Tais oportunidades e riscos criados pela digitalização fazem imperativa a necessidade de se criarem precauções para a proteção do bem-estar não apenas individual, como também do coletivo. Para tanto, todos os atores envolvidos podem e devem agir, aí incluídos os provedores de aplicações.

Hoffmann-Riem (2022, p. 254-255) pontua que a transformação digital também produz efeitos sobre a estrutura das responsabilidades, de modo que é plenamente possível pensar em transferência do poder de agir para instituições privadas nos setores caracterizadas pela digitalização, sem prejuízo da atuação do Estado como garantidor do bem individual e coletivo:

> Em muitas áreas, pode-se observar a retirada do direito público como meio de moldar as condições de vida. Não só, mas especialmente sustentável é a transferência do poder de agir para instituições privadas nas áreas caracterizadas pela digitalização. Em muitos casos, os atores agem de acordo com diretrizes autodefinidas e geralmente definidas e aplicadas unilateralmente, mesmo que terceiros – como os usuários de seus serviços – sejam afetados.
> Os particulares – protegidos pelas liberdades civis – são, em princípio, livres para perseguir seus interesses e especificar seus cálculos de benefício. No entanto, não estão completamente isentos de consideração pelos interesses dos outros e pelo bem comum. Se necessário, a lei pode ou deve estabelecer uma estrutura para garantir o exercício socialmente aceitável da liberdade. A grande importância da autodeterminação privada e da autorregulação não altera, portanto, a tarefa do Estado como "Estado garantidor" de assumir uma "responsabilidade garantidora" pela salvaguarda do bem individual e comum também por lei (grifo nosso).

Vale o alerta de Hoffmann-Riem, a resposta deve ser procurada dentro do ordenamento nacional. Essa responsabilidade das companhias tecnológicas, esse dever de agir, deve estar constitucionalizada no Brasil e efetivamente está.

## 2.2 DEVERES FUNDAMENTAIS COMO FERRAMENTA DE EFETIVAÇÃO DE DIREITOS FUNDAMENTAIS

### 2.2.1 Aspectos introdutórios

No meio jurídico, o só fato de se fazer menção ao tema deveres fundamentais, por vezes, já suscita algumas reações peculiares, destacando-se aquelas representativas de um absoluto desconhecimento da temática específica, bem como aquelas normalmente acompanhadas por olhares e palavras de desconfiança.

E não é para menos, como bem observa Colnago (2014, p. 398):

> Enquanto a palavra “deveres” é usada apenas nove vezes no Texto Constitucional de 1988, a expressão “direitos” surge em 98 ocasiões. Referida disparidade não é mera coincidência, na medida em que o paradigma do constitucionalismo que vivenciamos tem sua base na airmação de direitos e não na imposição de deveres.

O tema dos deveres fundamentais é manifestamente um dos menos estudados pelos constitucionalistas, recebendo pouca ou quase nenhuma atenção da doutrina constitucional contemporânea, nacional e estrangeira. As razões por trás dessa constatação se inserem no amplo contexto do desinteresse pela compreensão teórica das posições jurídicas passivas, ou estados de sujeição dos indivíduos (deveres e obrigações) no âmbito do direito público, o que em muito se deve ao próprio desenvolvimento da noção de estado de direito. Isso porque, segundo Casalta Nabais (2002, p. 16), o processo de formação da ideia de Estado de direito se conecta com o histórico de lutas sociais, que, justamente para imprimir maior relevo na demarcação dos limites do poder do Estado, acabou por se concentrar mais enfaticamente no reconhecimento e na afirmação das posições jurídicas ativas dos particulares em face do Estado, a conferir proeminência à proteção da liberdade e da autonomia individuais.

Historicamente, no Brasil, o estudo dos deveres fundamentais foi deixado em segundo plano pelos pesquisadores e estudiosos da área, que tradicionalmente muito se importaram em se

debruçar nos estudos quanto aos direitos fundamentais, que, se por um lado, são essenciais para que se possa falar numa vida digna, não retiram a importância dos primeiros para que este mesmo desiderato seja alcançado, mormente diante do fato de ser um dos objetivos da República Federativa do Brasil a constituição de uma sociedade solidária, conforme art. 3º, I, da CF.

Nesse contexto, mostra-se impensável idealizar um Estado Democrático de Direito onde não existam deveres fundamentais a serem observados, aqui entendidos nos moldes em que conceituados no âmbito do Grupo de Pesquisa "Estado, Democracia Constitucional e Direitos Fundamentais" (GPEDDF), ligado ao Programa de PósGraduação Stricto Sensu da Faculdade de Direito de Vitória (FDV), como sendo "[...] uma categoria jurídico-constitucional, fundada na solidariedade, que impõe condutas proporcionais àqueles submetidos a uma determinada ordem democrática, passíveis ou não de sanção, com a finalidade de promoção de direitos fundamentais" (Fabriz; Gonçalves, 2013, p. 87-96), os quais impõem aos brasileiros natos e naturalizados, aos estrangeiros que no Brasil se encontrem, bem como às pessoas jurídicas nacionais ou estrangeiras que no território brasileiro desempenham suas atividades, a observância de padrões de conduta pautadas na solidariedade e que se voltem para que todas as pessoas possam desfrutar de uma vida digna, nos moldes em que garantido pelo art. 1º, III, da CF.

Em razão de serem pautados na solidariedade, para que existam, os deveres fundamentais nem sequer precisam estar insculpidos de maneira expressa em normas constitucionais, uma vez que eles decorrem da própria condição gregária dos seres humanos. Para conseguirem se desenvolver de maneira digna, os indivíduos precisam estar inseridos em dado contexto social, ou seja, precisam se relacionar com outras pessoas também detentoras de direitos e deveres fundamentais. Logo, as ideias de liberdade e de solidariedade, que legitimam respectivamente direitos e deveres fundamentais, devem conviver (Nabais, 2002, p. 24).

A mesma solidariedade que fundamenta a existência dos deveres fundamentais também possibilita que eles sejam, em muitos casos, autoaplicáveis, de modo que não se faz necessária a presença de regulamentação infraconstitucional para fins de que possamos reconhecer, por exemplo, a presença do dever fundamental de não transgredir a privacidade alheia, bem como de não causar danos ao meio ambiente.

Entre nós, portanto, não faz sentido exigir que, para que se possa falar em eficácia dos deveres fundamentais, deva haver a atuação do Poder Legislativo, pelo contrário, muitos desses deveres são implícitos e correlatos a direitos fundamentais insculpidos em nossa Carta Magna, enquanto outros se extraem do texto constitucional sem depender de integração legislativa, tal como o dever de colaborar com a segurança pública adiante abordado, não obstante existam deveres que demandem a atuação do legislador constituído, assim como ocorre com o dever de pagar tributos.

A exigência de leis regulamentadoras dos deveres fundamentais fica, dessa forma, restrita "[...] para aqueles comportamentos que necessitam de forma própria para se assegurar a proporcionalidade e isonomia [...]" (Fabriz; Laranja; Pedra, 2020, p. 263), em que a atuação legislativa dos representantes eleitos pelo povo se faz necessária para dar legitimidade aos deveres, tal como ocorre com o dever de pagar tributos, conforme elencado, que deve ter balizado por lei, dentre outros aspectos: seus fatos geradores, bases de cálculo e alíquotas.

Nessa linha de raciocínio, em se tratando dos deveres fundamentais de colaboração com a segurança pública e de cooperação judicial, quando não envolverem interferência nos princípios da proporcionalidade e da isonomia, não há que se falar em necessidade de regulamentação legal para que devam ser observados. Não é necessário lei para que se extraia que aquele que presencia um crime sem ser visto pelo transgressor tenha o dever de colaborar com a segurança pública, explicitando os envolvidos e as circunstâncias do delito, mormente diante da possibilidade de se fazer uso do anonimato para tanto; assim como que aquele que possui determinado documento que sirva de prova em litígio envolvendo terceiros deve apresentá-lo quando instado a tanto para se desincumbir de seu dever de cooperação judicial, principalmente quando tal conduta não envolver restrição de direitos fundamentais que mereçam tutela no caso concreto.

Em última análise, a autoaplicabilidade dos deveres fundamentais, quando não ocorra interferência no âmbito da proporcionalidade ou isonomia, decorre da própria necessidade de se dar efetividade aos direitos fundamentais a eles correlacionados (Pedra, 2013), haja vista que, sem a efetivação de ambos, não há que se falar em vida digna, sendo que a discussão acerca desta última categoria não pode deixar relegada ao reconhecimento da primeira.

Não obstante, convém mencionar que a intermediação do legislador será necessária para imposição de sanção por descumprimento de algum dever, pois normalmente tais sanções não são previstas no texto constitucional. Vale destacar que a sanção é importante, porque é um elemento coercitivo, mas não é imprescindível para a eficácia de um dever fundamental.

Os deveres fundamentais e os direitos fundamentais se complementam uns aos outros, não havendo então que se falar em Estado Democrático de Direito sem que se reconheça a presença dos dois institutos, de modo que, tendo a República Federativa do Brasil o objetivo de constituir uma sociedade solidária, não há como se ter êxito nessa meta sem que se reconheça a existência de deveres fundamentais.

Nesse cenário, quando a Constituição afirma, em seu art. 144, caput, ser a segurança pública não apenas direito, mas também responsabilidade de todos, estamos diante de autêntico dever fundamental decorrente da solidariedade, o mesmo ocorrendo com o dever fundamental de cooperação judicial que, além de decorrer de nossa Carta Magna, ganhou força com a promulgação do atual Código de Processo Civil (CPC) em 2015 e a previsão expressa em seu art. 6º (Buarque; Pedra, 2016).

Importante frisar que, quanto aos direitos fundamentais, admite-se que eles são dotados de eficácia horizontal para fins de incidirem nas relações entre particulares de maneira direta (Vello; Pedra, 2011), haja vista que o balizamento desses tipos de relacionamento também se faz imprescindível para fins de que se alcance uma vida digna, mormente se considerada as diferenças técnicas, informacionais e econômicas que pode haver entre os envolvidos.

A mesma lógica deve ser estendida aos deveres fundamentais, de forma que reconheçamos que não apenas perante o Estado existem deveres fundamentais a serem observados, mas também nas relações entre particulares, até pelo fato de que determinados ônus estatais são repassados para estes, isso sem contar a importância que os deveres possuem para o asseguramento de uma vida digna, que deve ser respeitada em todos os âmbitos.

A título exemplificativo, não podemos descurar que, nas relações de consumo, assim como nas relações entre pais e filhos, existem deveres a serem observados pelos particulares, os quais são embasados em valores coletivos que fogem às raias dos interesses meramente

privados[178], estando esses valores ligados à ideia de constituição de uma sociedade solidária, possuindo a envergadura de autênticos deveres fundamentais.

Traçado esse panorama de uma teoria geral dos deveres fundamentais, e sem descuidar que de forma correlata ao direito fundamental à privacidade também existe um dever fundamental de respeitá-la, inclusive na relação entre particulares, quadra analisarmos dois deveres fundamentais de grande importância para o presente trabalho já anteriormente citados, quais sejam: os deveres de cooperação com a justiça e de colaboração com o sistema de segurança pública.

### 2.2.2 Dever fundamental de cooperação com a administração da justiça

É bem verdade que, em relação ao dever fundamental de colaboração com a administração da justiça, não há previsão expressa dele a nível constitucional, o que não consiste em óbice para o seu reconhecimento, haja vista que se admite a presença de deveres fundamentais implícitos, sendo que o dever em comento pode ser facilmente extraído do art. 5º, LIV e LV, ambos da CF (Vello; Pedra, 2011), que trazem, respectivamente, o princípio do devido processo legal e o do contraditório e da ampla defesa.

Em decorrência desses dois princípios, podemos extrair que tanto as pessoas físicas como as jurídicas possuem o dever fundamental de colaborarem com a administração da justiça, de modo que elas não apenas possuem o direito de acioná-la quando necessitem assegurar tutelar à violação de direitos, mas também o dever de auxiliá-la, tal como testemunhando em processos judiciais, comparecendo em sessões de julgamento do Tribunal do Júri na qualidade de jurados e fornecendo documentos que detenham que sirvam como provas em processos envolvendo terceiros.

O cumprimento do dever fundamental dos particulares de colaboração com a justiça, sejam pessoas físicas ou jurídicas, é essencial para que esta possa ser prestada não apenas de maneira célere, nos moldes em que exigido pelo art. 5º, LXXVIII, da CF, mas também de maneira efetiva e de modo a não possibilitar que se tenham julgamentos lastreados na ausência de verdade acerca dos fatos em análise, tanto no âmbito cível, como no criminal. “Assim, ao dever do Estado de prestar uma jurisdição.

justa, adequada, célere e eficaz atrela-se o dever das partes de cooperarem entre si com o mesmo objetivo" (Buarque; Pedra, 2016, p. 113), mas não somente destas, pois também de todos os sujeitos processuais, inclusive dos terceiros que possam de algum modo participar dessa relação.

Saliente-se que, apesar do dever fundamental de colaboração com a justiça ser extraível diretamente da Constituição, ele ganhou ainda mais força com o advento do atual Código de Processo Civil, promulgado em 2015, o qual prevê, em seu art. 6º, que todos os sujeitos do processo, e não apenas as partes, devem colaborar com o desenvolvimento dos processos judiciais para que se possa chegar a uma decisão justa (Brasil, 2015).

### 2.2.3 Dever fundamental de contribuição com a segurança pública

Assentada a existência de um dever fundamental de colaboração com a justiça, importante frisar que, ao mesmo tempo em que a Constituição elenca a segurança pública como sendo um direito, ela em contrapartida aduz, em seu art. 144, caput, que todos têm a responsabilidade de colaborar para que ela realmente ocorra, para que assim seja resguardada a paz social, bem como a incolumidade física e patrimonial que tanto desejamos.

Por mais que a Constituição faça uso da denominação "responsabilidade", e não "dever", diante do fato de os deveres fundamentais se basearem na solidariedade, as pessoas, sejam físicas ou jurídicas, também possuem o dever de colaborar com a segurança pública, seja participando na formulação de políticas afetas à área e em suas fiscalizações, bem como levando ao conhecimento de autoridades ligadas à persecução penal informações que digam respeito à prevenção e repressão à prática de infrações penais, quando a adoção de mencionada conduta não as colocarem em risco.

O fato de se dizer que todos possuem o dever fundamental de colaborar com a segurança pública não significa que estejam compelidos a enfrentar diretamente à criminalidade, até pelo fato de que o adimplemento de deveres fundamentais não pode importar em sacrifício ou colocação de direitos fundamentais dos devedores em risco de maneira desarrazoada, desproporcional, excessiva ou exorbitante (Pedra, 2013, p. 287).

Mas também não se pode conceber a constituição de uma sociedade solidária onde, em situação que não envolva risco, a integridade física e até mesmo a vida de pessoa que tenha acesso a informações importantes para prevenção ou elucidação de infrações penais, não seja reconhecido um dever fundamental desta de colaborar como a segurança pública e até mesmo com a justiça criminal, que acaba por ser também uma decorrência do primeiro dever.

Nesse contexto, se por um lado a efetivação do direito fundamental à segurança pública, ligada à manutenção da ordem pública interna (Silva, 2009), em todos os seus aspectos demanda a adoção de posturas positivas por parte do Estado, tais como estruturar os órgãos de segurança pública listados no art. 144 da CF e combater diretamente através de seus agentes a criminalidade, por outro, para que esse direito possa ser assegurado, necessário também se faz o reconhecimento do dever fundamental dos particulares colaborarem com ela, assim como ocorre com aquele que detenha documentação ou informação que elucide infrações penais, sem que o seu fornecimento às autoridades implique qualquer assunção de risco desarrazoado.

Feitos esses esclarecimentos, insta investigarmos se a utilização da criptografia de ponta a ponta e a proteção ao direito fundamental à privacidade que ela confere é compatível com os deveres fundamentais de colaboração com a justiça e com a segurança pública.

## 2.3 DEVERES FUNDAMENTAIS DOS PROVEDORES DE APLICAÇÃO DE CONTRIBUIR COM A SEGURANÇA PÚBLICA E A COOPERAÇÃO COM A ADMINISTRAÇÃO DA JUSTIÇA

Diante da revolução 4.0 que vivenciamos, mostra-se inegável a importância e a influência que artefatos tecnológicos ganham em nossas vidas, sendo que os aparelhos celulares, por poderem ser facilmente transportados, permitem nossa conexão com o mundo de onde quer que estejamos.

Hodiernamente se torna cada vez mais difícil encontrar alguém que não possua um aparelho celular que permita conexão com a internet, o que consequentemente eleva a quantidade de usuários de aplicações como ferramentas de comunicação e de negócios.

Ocorre que, se por um lado os aplicativos de mensageria permitem a interação social entre pessoas que não se fazem presentes, bem como permite o entabulamento de negócios de índole profissional ou empresarial, por outro também vêm sendo utilizados para preparação ou como instrumento destinado à prática de delitos, mormente se considerada sua potencialidade para dificultar alguns tipos de investigação em decorrência da utilização de criptografia de ponta a ponta.

Como dito (item 2.3), o direito à privacidade também deve ser entendido como norma de bloqueio, destinada a assegurar ao indivíduo a existência de espaços livres de interferência alheia, razão por que existirão direitos e deveres correspondentes tanto para potenciais violadores desses espaços, como também para aqueles que possuam o dever jurídico de protegê-los (sejam agentes públicos ou privados).

Ademais, considerando-se que, assim como os direitos fundamentais, os deveres fundamentais também são dotados de eficácia horizontal para fins de incidirem nas relações entre particulares, tem-se os provedores de aplicação, entidades privadas fornecedoras de serviços que são, têm o dever de observar e proteger a privacidade de deus usuários, garantindo, na maior medida possível, a confidencialidade das comunicações em fluxo e dos dados particulares armazenados contra os riscos de devassa.

Porém, a utilização dessa forma de criptografia permite, por outro lado, que infrações penais sejam praticadas no âmbito desse mecanismo de comunicação, sem que se possa ter acesso ao teor das conversas dos usuários, o que o potencializa como palco para a prática e preparação de delitos.

Ocorre que, do mesmo modo que a privacidade figura como direito fundamental previsto no art. 5º, X, da Constituição, a segurança pública também possui idêntica natureza, nos termos do art. 6º da CF, sendo que o art. 144 a eleva como sendo de responsabilidade de todos.

Não obstante normalmente radicados no estrangeiro, os provedores de aplicação possuem atuação no Brasil e, como tais, são detentores de direitos e garantias de índole constitucional, como o direito de ter seu patrimônio protegido contra atividades criminosas.

Em contrapartida, provedores de aplicação também possuem deveres fundamentais a serem observados, que não se limitam à proteção da privacidade dos usuários do aplicativo, indo muito além, gerando, no que interessa a este trabalho, o dever de colaborar com o sistema de segurança pública, bem como com o desenvolver de processos judiciais quando forem instados a colaborar com a justiça (art. 6º do CPC, c/c art. 5º, LIV, da CF). Quanto ao último dever, como bem frisado por Rodrigo Costa Buarque e Adriano Sant'Ana Pedra (2016, p. 115):

> No atual contexto de Estado Democrático de Direito faz-se necessário valorizar a participação social, visando à obtenção de uma solução racionalmente justificada aos difíceis casos decorrentes do conflito social. No campo processual esta visão implica na necessidade de cooperação, a ser exigida dos sujeitos processuais.

O problema que surge é de como compatibilizar o dever de proteção da privacidade de seus usuários com os deveres fundamentais de colaborar com o sistema de segurança pública (Grobério; Pedra, 2022, p. 128) e com o desenrolar de processos judiciais. Certamente a criptografia de ponta a ponta surge como grande empecilho a mencionado desiderato, uma vez que não permite a recuperação, a interceptação e o compartilhamento das mensagens ligadas à preparação, execução ou consumação de crimes que tenham sido trocadas dentro do aplicativo (Santos; Faure, 2019, p. 61).

No caso de investigações que objetivem alcançar conversas travadas em aplicativos de mensageria, para se ter acesso ao conteúdo de mensagens de algum criminoso, as autoridades ligadas à persecução penal ainda precisariam contar com a sorte de obter sucesso na apreensão do dispositivo eletrônico do infrator. Afora as eventuais dificuldades de recuperação de conversas apagadas, antes disso ainda seria necessário o acesso ao dispositivo desbloqueado, o que esbarra na necessidade de cooperação do investigado ou na disponibilidade de tecnologia para a superação da proteção criptográfica.

Importante frisar que, mesmo no cenário narrado, na ausência de consentimento do proprietário do telefone apreendido, necessária será a obtenção de autorização judicial para a devassa no aparelho telefônico apreendido, não podendo ser outro o caminho, à luz do disposto no art. 5º, XII, da CF e da proteção constitucional à privacidade, que se encontra intrinsecamente ligada à existência de uma vida digna.

Reforçada fica a possibilidade de que os provedores de aplicações de mensageria tenham que cumprir o seu dever de colaborar com a segurança pública quando acrescido o dever que eles também possuem de colaborar com o desenvolver de processos judiciais, conforme expressamente previsto no art. 6º do CPC e aplicável ao processo penal, na forma do art. 3º do CPP (Fischer, 2016, p. 52).

Aludindo a companhias caracterizadas pela digitalização em geral, Hoffmann-Riem (2019, p. 541) alerta que, como inexistem "[...] estruturas regulatórias estatais de vigência global para os serviços na internet, as possibilidades de conformação organização autônoma são particularmente grandes para as empresas", o que faz com estas tenham responsabilidade própria pela conformação organizacional que atribuem aos seus modelos de negócios na internet. Inobstante, onde tais empresas (aí incluídos os provedores de aplicação de mensageria) mantiverem suas sedes empresariais, alguma filial ou exercerem suas atividades, elas estarão regidas pelo ordenamento jurídico que abranja respectivo território.

O entendimento tem guarida na ordem jurídica brasileira. O MCI estabelece a exigência de respeito à legislação brasileira em todas as operações de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet quando ao menos um desses atos ocorrer em território nacional:

> 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 e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
> § 1º O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.
> § 2º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.
> § 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações (Brasil, 2014).

O Código de Processo Civil[27], de igual modo, não deixa dúvidas que a jurisdição nacional incidirá quando (i) o réu mantiver domicílio, agência, filial ou sucursal no Brasil (qualquer que seja a sua nacionalidade); (ii) eventual obrigação tiver de ser cumprida no Brasil; e (iii) a pretensão se fundar em ato ou fato ocorrido em solo nacional (art. 21).

A Lei de Introdução às Normas do Direito Brasileiro (LINDB – Decreto-Lei nº 4.657, de 4 de setembro de 1942) é imperativa ao preconizar que as obrigações são regidas pelas leis do país em que elas se constituírem, sendo que, se alguma obrigação tiver de ser executada no Brasil, deverá seguir as exigências de forma contidas na legislação brasileira[28]. Assim, caso uma pessoa jurídica estrangeira pretenda se estabelecer e prestar os seus serviços (contraindo obrigações e titularizados direitos) de internet no Brasil, tem-se que deverá estar constituída de acordo com o ordenamento jurídico interno para que possa realizar regularmente suas operações no território nacional. Satisfeita essa condição, a pessoa jurídica estará inevitavelmente sujeita à jurisdição brasileira e não poderá se negar a dar cumprimento a decisões judiciais válidas do Poder Judiciário. Incidirá a jurisdição nacional sempre que for o caso de fornecimento de dados digitais originados a partir do território brasileiro. Corroborando o raciocínio, Fernanda Domingos e Priscila Röder (2017, p. 55) anotam que:

> Assim, uma conta-corrente bancária, aberta numa instituição financeira estabelecida em território nacional e, portanto, constituída sob as leis brasileiras, (nos termos do Decreto-Lei nº 4.657 de 4 de setembro de 1942, Lei de Introdução às Normas do Direito Brasileiro – LINDB) está sujeita a ter seus documentos e informações apresentados ao juiz brasileiro, mesmo que tais informações estejam arquivadas em uma filial ou matriz da instituição financeira situadas no exterior. Por outro lado, uma conta-corrente bancária aberta no exterior, isto é, sob a soberania e jurisdição de outro Estado, somente terá seus dados e informações disponibilizados ao Judiciário brasileiro mediante pedido de cooperação internacional, mesmo que tal instituição financeira possua congênere no território brasileiro, pois neste último caso o serviço, ou seja, a abertura da conta-corrente e sua manutenção, não foi prestado em território nacional, mas sim no Estado estrangeiro.

Firmada a premissa de que os provedores de aplicação têm o dever fundamental de contribuir com a segurança pública e de cooperar com a administração da justiça, e tendo em conta que é inegável que a persecução penal é negativamente impactada pelo uso da criptografia como medida antiforense, como se viu ao expor o debate desenvolvido nas guerras criptográficas,

[27] De aplicação subsidiária ao Código de Processo Penal, por força do seu artigo 3º e do artigo 4º da Lei de Introdução às Normas do Direito Brasileiro.

[28] "Art. 9º Para qualificar e reger as obrigações, aplicar-se-á a lei do país em que se constituírem. § 1º Destinando-se a obrigação a ser executada no Brasil e dependendo de forma essencial, será esta observada, admitidas as peculiaridades da lei estrangeira quanto aos requisitos extrínsecos do ato" (BRASIL. Decreto-Lei nº 4.657, de 4 de setembro de 1942. Brasília, 1942. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del4657.htm. Acesso em: 10 dez. 2022).

cabe perquirir de quais maneiras os provedores de aplicações podem de desincumbir dos seus ônus. Teriam eles o dever impor mecanismos que de alguma forma fragilizassem a criptografia? Decerto que não. É o que se verá no tópico seguinte.

## 2.4 A ESSENCIALIDADE DA CRIPTOGRAFIA COMO FERRAMENTA DA PROTEÇÃO DE DADOS: PROBLEMAS E CONSEQUÊNCIAS DE EVENTUAL FLEXIBILIZAÇÃO

Ao cabo de aproximadamente 30 anos de cryptowars, consolidou-se relativo consenso no sentido de que qualquer mecanismo de acesso excepcional implica a fragilização das proteções propiciadas pela criptografia como um todo (Aranha, 2018; Habelson et al., 2018; ONU, 2015; Liguori, 2022; Razera, 2021). Tal fragilização se revela em duas constatações centrais: (i) o acréscimo de mecanismos de acesso excepcional ao conteúdo criptografado ocasiona a ampliação da superfície de ataque [29] (seja porque as interações entre as características adicionadas podem gerar vulnerabilidades, seja porque o meio de acesso excepcional pode ser descoberto por agentes mal-intencionados); e (ii) qualquer banco de dados que concentre uma enormidade de chaves criptográficas de usuários se transforma, inevitavelmente, em alvo perfeito de ataques por indivíduos e entidades mal intencionados (Souza Abreu, 2017, p. 38).

A segunda constatação é autoexplicável, cabendo alguns esclarecimentos em relação à primeira. É que, quanto mais simples é um sistema criptográfico, menos sujeito a vulnerabilidades ele fica. Dito de outro modo, a complexidade de sistemas criptográficos é inversamente proporcional à segurança nele existente. Destarte, com a implementação de qualquer mecanismo de acesso excepcional, ter-se-á, como consequência, o aumento da complexidade do sistema, já que serão inseridas novas funções antes não existentes (Aranha, 2018, p. 31). Novas funções que impliquem a vulnerabilidade do sistema, como o encaminhamento de chaves para autoridades, poderão ser descobertas por agentes mal-intencionados e desbordarão em inerente insegurança do usuário. Além disso, quanto mais

[29] "A superfície de ataque de um sistema é composta dos pontos passíveis de intervenção pelo atacante, incluindo protocolos de comunicação, mecanismos de autorização, processos humanos, algoritmos criptográficos e suas implementações em software ou hardware. [...] Calcular e armazenar chaves criptográficas apenas nas pontas da comunicação simplifica uma aplicação criptográfica porque torna evidente quais são os principais pontos que exigem proteção, reduzindo a ameaça de pontos intermediários ou atacantes internos que operam o serviço e desfrutam de acesso privilegiado. Apesar de a designação ter se tornado comum no mercado para aplicativos de troca segura de mensagens (WhatsApp, Signal, Wire etc.), a maioria dos protocolos criptográficos modernos pode ser classificada como fim a fim" (Aranha, 2018, p. 5).

características forem adicionadas a um sistema, maiores serão as chances de as interações entre elas ensejarem fragilidades:

> Quanto à intensificação dos riscos, destaca-se que a complexidade de sistemas é inversamente proporcional à sua segurança. Quanto maior o número de características adicionadas, maior a probabilidade de que a interação entre elas enseje vulnerabilidades. Um dos principais antídotos contra isso também fica comprometido - pela própria natureza do acesso excepcional, as funcionalidades voltadas a esse objetivo dificilmente passarão pelo escrutínio público da comunidade técnica que avaliza esses sistemas. Uma forma de o mercado responder a essa problemática pode ser justamente reduzindo a complexidade dos mecanismos de proteção, gerando um desincentivo a tecnologias mais seguras e preocupadas com a privacidade desde seu design (Alimonti, 2020).

Tendo em conta que as preocupações das autoridades de aplicação da lei não se voltam especificamente à crescente propagação de sistema de criptografia ponta a ponta, mas sim ao seu uso na proteção da comunicação entre indivíduos, notadamente diante dos problemas (medida antiforense) que cria às apurações de crimes de alguma forma conectados a essa tecnologia, verifica-se que eventuais "soluções" para indigitadas dificuldades perpassam pelo exame da necessidade e da adequação da implementação de mecanismos de acesso excepcional aos fins pretendidos, porquanto direitos fundamentais como a privacidade e a liberdade de comunicação (dentre outros) serão atingidos pela medida interventiva.

Relativamente aos aplicativos de mensageria privada (em que a criptografia de ponta a ponta é regra), nota-se que normalmente eles vêm acompanhados de outras ferramentas de segurança para detecção de iniciativas maliciosas de acesso, a exemplo da autenticação em dois fatores[30], as quais obstariam de plano eventuais investidas. Com isso, tais ferramentas deveriam ser desabilitadas para permitir o acesso ao sistema, o que seria fatalmente notado por agentes com mínima sofisticação em suas ações. Ademais, iniciativas de fragilização dos sistemas de segurança de aplicativos de mensageria mais cedo ou mais tarde repercutiriam na mídia e provocariam, em alguns cenários, o próprio abandono do uso de determinada aplicação[31], sobretudo daqueles interessados em fazer da criptografia forte medida antiforense de ocultação de suas ações e provas. Como alerta Aranha (2018, p. 11):

---

[30] "A autenticação de dois fatores é uma camada extra de segurança na conta, que tem como objetivo confirmar a identidade do usuário. Ao ativar a verificação em duas etapas, o usuário precisa fornecer uma segunda informação após inserir login e senha, e só então terá acesso à conta" (Disponível em: https://www.techtudo.com.br/noticias/2021/08/autenticacao-de-dois-fatores-o-que-e-e-para-que-serveo-recurso.ghtml. Acesso em: 4 out. 2022).

[31] Após um ataque terrorista em Mumbai, Índia, no ano de 2008, em que se descobriu que os terroristas faziam uso de celulares BlackBerry (um dos primeiros smartphones com criptografia forte para comunicações), a fabricante "Research in Motion" (RIM), cedeu, em 2012, às ameaças de banimento do Governo indiano e

> Partes comunicantes que empregam o mínimo de boas práticas ao utilizar esses produtos têm plena capacidade, por projeto, para detectar a interferência indevida e descartar a comunicação. A própria repercussão na mídia sobre possível intervenção do aparato investigativo sobre esses produtos provoca efeito contrário ao esperado pelo esforço de interceptação legal: os usuários, quaisquer que suas naturezas ou objetivos, aprimoram sua segurança operacional e se tornam mais vigilantes quanto a interferências indevidas. Pode se imaginar, portanto, que, para ser eficaz, o esforço de interceptação legal obrigatoriamente precise vir acompanhado de um conjunto de medidas que desabilitem mecanismos de detecção disponíveis aos usuários, degradando progressivamente a segurança do produto ou protocolo. Esse é um caminho sem volta em uma espiral descendente, que obriga a introdução de falhas intencionais cada vez mais profundas para preservar o caráter indetectável do mecanismo de interceptação [...].
>
> Como usuários minimamente equipados com informação técnica já são capazes de detectar a interferência indevida, é absolutamente plausível esperar que os agentes sob investigação procurem tomar cuidados equivalentes. Suspeitos sem nenhuma sofisticação técnica talvez possam ser monitorados com sucesso utilizando o mecanismo de interceptação legal, mas é racional assumir que existam outras maneiras menos intrusivas de fazê-lo. Suspeitos com alguma sofisticação técnica deverão aprimorar suas práticas de segurança proporcionalmente e possivelmente evitem utilizar aquela plataforma em particular, migrando para outros meios de comunicação mais sutis e afastados da capacidade de monitoração do aparato investigativo. Suspeitos com alta sofisticação técnica muito provavelmente construirão suas próprias plataformas ultrassigilosas de comunicação, a partir de informação publicamente disponível. Não há obstáculo técnico insuperável em um esforço dessa natureza, visto que as técnicas subjacentes são dominadas há décadas e há aplicativos de código aberto que implementam as mesmas técnicas de criptografia fim a fim que podem ser facilmente adaptados para funcionar utilizando infraestrutura dedicada própria.

Ainda tratando de aplicativos de mensageria, uma questão que merece atenção é a da eficácia social de restrições à criptografia em caso de descumprimento das normas de regência, inegavelmente dotadas de eficácia jurídica. Em sendo o caso de decretação de bloqueio de uma aplicação dentro de uma determinada jurisdição, a medida poderia ser contornada mediante o uso de meios alternativos de acesso a aplicações, a exemplo de VPNs ou da rede Tor [32]. Entre nós, a grande aderência da sociedade ao compartilhamento ilícito de filmes por

---

instalou um dos seus servidores em Mumbai, viabilizando um mecanismo de acesso excepcional a dados de usuários (SWIRE, Peter; AHMAD, Kenesa. Encryption and Globalization. The Columbia Science & Technology Law Review, v. 13, 2011, p. 419 e 443). A implementação do referido mecanismo marcou a queda das vendas de aparelhos BlackBerry, abrindo espaço ao mercado para a alavancagem da venda de smartphone das concorrentes, como Apple e Samsung. Para mais informações, ver: https://www.tecmundo.com.br/blackberry/47677-como-ablackberry-enterrou-o-seu-imperio-no-mercado-de-smartphones-.htm. Acesso em: 9 out. 2022. Entre nós, um fato reforça especialmente essa conclusão, que foi o grande aumento do número de usuários do Telegram, que se popularizou ainda mais após o bloqueio do WhatsApp. Conforme anúncio da plataforma, após poucos dias que se seguiram à ordem de bloqueio do maior concorrente, o Telegram recebeu aproximadamente um milhão e meio de novos usuários (Disponível em: https://exame.com/tecnologia/telegram-ganha-1-5-mi-de-usuarios-com-bloqueio-de-whatsapp/. Acesso em: 14 out. 2022). O fato repercutiu de forma tão acentuada que chegou a ser citado por Van Hoboken Schulz, em seu relatório sobre direitos humanos e encriptação publicado pela UNESCO em 2016.

[32] VPN e rede Tor são meios de anonimização na internet, ao lado da criptografia.

meio da internet retrata bem o problema de ineficácia social da norma jurídica (AiotBrasil, 2022).

Com efeito, a despeito de a inserção de mecanismos de acesso excepcional aparentar que produzirá reflexos pontuais, o que se nota que é, ao serem inseridas vulnerabilidades intencionais em sistemas criptográficos para viabilizar investigações e repressão de crimes, o que se obtém é a redução da segurança desses sistemas, os quais foram criados exatamente para proteger a privacidade e prevenir que seus usuários sejam vítimas de crimes, não obstante terminem por também resguardar criminosos.

Ainda que se pretenda a criação de falha para alcançar apenas investigados certos e determinados, sabe-se que a vulnerabilidade pertence ao sistema e, por isso, alcança todos os seus usuários (a porta que se abre para um fica igualmente aberta para todos), haja vista que os aplicativos de mensageria com criptografia funcionam em nível global e não local[33]. Com isso, os riscos de vazamento de dados a partir da exploração de vulnerabilidades se elevariam (Altieres, 2017).

A projeção global desses serviços também redunda em claras dificuldades de coordenação entre provedores de aplicação e as múltiplas autoridades dos inúmeros países do mundo, vários deles com viés autoritário. O cenário parece ir na contramão da razão essencial do aprimoramento das tecnologias da informação, que é obstar a vigilância e proteger a privacidade e a segurança do usuário.

Rememore-se, ademais, que policiais, promotores, juízes, além de outras autoridades também não escapariam dos efeitos negativos da implementação de mecanismos de acesso especial. O lamentável caso denominado Vaza Jato (Greenwald, 2019) ensinou uma poderosa lição acerca dos possíveis efeitos negativos de vulnerabilidades do aplicativo Telegram para a comunicação de autoridades estatais. Não bastasse, a segurança de provas e dados digitais de

[33] Nesse sentido: “Quando lembramos que um mesmo serviço de comunicação costuma ser utilizado em vários países e que as comunicações via internet quase sempre atravessam fronteiras, podemos perceber como a regulação da criptografia em um país pode criar uma falha de segurança que afeta todos os outros que utilizam um mesmo sistema de comunicação. Se um país proíbe criptografia eficaz ou impõe vulnerabilidades aos serviços utilizados em seu território, então a comunicação que parte desse país ou passa por sua infraestrutura estará necessariamente menos segura. Afirma-se, nesse sentido, que um sistema de comunicação internacional é tão seguro quanto o país mais restritivo envolvido permite que ele seja” (Liguori, 2022, p. 282-283).

interesse de órgão de investigação também seria impactada com o enfraquecimento da criptografia.

Tendo em vista os vários efeitos negativos da inclusão de vulnerabilidade intencional, verifica-se que o meio é inadequado aos fins a que se propõe, afora a existência de alguns meios menos intrusivos de investigação, como o acesso a metadados e dados armazenados em nuvens.

Em suma, a fragilização da criptografia em aplicativos de mensageria instantânea tem o condão de impactar negativamente não apenas os indivíduos, como os governos e as próprias autoridades de aplicação da lei, terminando por vulnerar, em última instância, a proteção de uma vasta gama de direitos fundamentais, como a privacidade, a proteção de dados, as liberdades de comunicação, de opinião, expressão, econômica, entre outros relacionados direta ou indiretamente com esses.

## 2.5 PARA ALÉM DA METÁFORA DA ESCURIDÃO: AS FORMAS ALTERNATIVAS DE INVESTIGAÇÃO

São muitas as vozes que se levantam para alertar sobre duvidosas vantagens e os graves danos que podem recair sobre diversos direitos fundamentais em caso de enfraquecimento, por qualquer modo, das proteções criptográficas.

Em suma, a criptografia é essencial às modernas condições de vida. É preciso mudar o foco, retirar os holofotes das propostas de enfraquecimento da criptografia e voltálos à premente necessidade de adaptação das autoridades de investigação. Como medidas de adaptação, duas possibilidades despontam, dentre outras, para as autoridades de persecução: (i) a busca por meios, tecnológicos ou não, para superação das barreiras criptográficas e/ou (ii) a obtenção de dados estáticos contidos em suportes eletrônicos[34].

[34] Desde já, é possível identificar três características comuns que envolvem o acesso a esse grupo de dados: (i) não depende de expedientes para a superação de barreiras criptográficas, já que estão fora do ambiente com criptografia; (ii) podem ser cedidos desde logo para as investigações em curso, dado que inexiste, como regra, óbice técnico; e, como dito, (iii) pressupõe a colaboração dos provedores de aplicação na entrega dos dados e metadados.

Na primeira hipótese, incluem-se medidas que vão desde a obrigação de fornecimento de senha ou biometria pelo investigado ou terceiros (suscitando sopesamento da garantia da não autoincriminação) até o emprego de técnicas de "hacking governamental", isto é, técnicas de exploração de vulnerabilidades preexistentes em sistemas ou uso de outras ferramentas[35] de hacking para buscar e acessar dados e informações legíveis em suportes eletrônicos protegidos. Trata-se de soluções muito debatidas[36] mundo afora, quando se fala das novas fronteiras das investigações criminais. A par de receberem tanto críticas como aplausos dos atores envolvidos nas discussões, é certo que várias delas vêm sendo positivadas e praticadas em algumas ordens jurídicas[37][210], projetando-se como possíveis alternativas[38] de longo prazo no caso do Brasil (dado o atual contexto legislativo quanto ao ponto).

---

[35] A solução "UFED" da empresa Cellebrite é exemplo de tecnologia que viabiliza a extração e análise de todo conteúdo digital em dispositivos eletrônicos como smartphones, tablets ou aparelhos GPS de suspeitas ou vítimas de crimes. Vide: https://sisnema.com.br/policia-federal-adota-cellebrite-parainvestigacao-da-lava-jato. Acesso em: 4 out. 2022. Para mais informações sobre os produtos da empresa, vide o sítio eletrônico da empresa TechBiz Forense Digital, distribuidora das ferramentas Cellebrite (Disponível em <Chttps://techbiz.com.br/. Acesso em: 4 out. 2022)

[36] Em um relatório do ano de 2017, elaborado pelo Gabinete do Diretor de Inteligência Nacional dos EUA, são apresentadas algumas alternativas para a superação das dificuldades das autoridades de persecução. Dentre elas, estão o fortalecimento das técnicas de hacking governamental e a realização de parcerias com as empresas de tecnologia para viabilizar o intercâmbio dos meios de provas com as autoridades de persecução (MITCHELL, Bonnie et al. Going Dark: Impact to Intelligence and Law Enforcement and Threat Mitigation. 2017. Disponível em: https://cyberwar.nl/d/fromDNI.gov/10---2017AEP_Going-Dark.pdf. Acesso em: 31 set. 2022).

[37] Uma das formas "hacking governamental" para fins de persecução foi regulamentada recentemente na Alemanha sob a modalidade infiltração em dispositivo eletrônico. Segundo Orlandino Gleizer, "reforma consistiu, principalmente, em dar autorização para uma específica medida cuja legalidade era há muito tempo controversa: o monitoramento de telecomunicação na fonte (TKÜÜberwachung). Isso foi necessário – e serve como um bom exemplo do rigor de uma garantia de reserva de lei consequente – porque alguns métodos de telecomunicação por softwares que garantem criptografia (como o Skype) por meio de sistema VoIP (voice over IP) exigiam uma medida adicional, a infiltração de sistemas informáticos.". (grifos nossos). Assim dispõe a Seção 100(a) do Strafprozeßordnung (Código de Processo Penal alemão): "§ 100a Monitoramento de telecomunicação (1) Sem o conhecimento do afetado [ocultamente], pode-se, monitorar e gravar a telecomunicação, caso 1. fatos determinados fundamentem a suspeita de que alguém consumou ou, caso a tentativa seja punível, tentou consumar como autor ou partícipe ou, por meio de um crime, preparou um crime grave, listado no rol da Abs.2, 2. o crime seja especialmente grave também no caso concreto e 3. a investigação dos fatos ou do local onde se encontra o imputado fosse, de outro modo, consideravelmente mais difícil ou infrutífera. O monitoramento e gravação da telecomunicação também pode ocorrer por meio de intervenção, com meios técnicos, em sistema informático utilizado pelo imputado, caso isso seja necessário, para possibilitar o monitoramento e gravação, especialmente, em forma descriptografada. Os conteúdos e as informações da comunicação armazenados no sistema informático do imputado só podem ser monitorados e gravados, caso eles, durante o processo de telecomunicação, também pudessem ter sido monitorados e gravados, em forma criptografada, em rede de telecomunicação pública. (2) Crimes graves no sentido da Abs. 1 nr. 1 são: 1. do Código Penal: a) crimes de alta traição e de perigo para o estado democrático de direito... b) corrupção ativa ou passiva de mandatório da federação ou dos estados... c) crimes contra a defesa nacional... d) crimes contra a ordem pública... e) falsificação de moedas... f) crimes contra a autonomia sexual... g) pornografia infantil... h) homicídio e homicídio qualificado... i) crimes contra a liberdade pessoal (tráfico de pessoas... prostituição compulsória... escravidão...) j) furto em bando... k) roubo e extorsão... l) crimes de receptação... m) lavagem de dinheiro... n) estelionato e estelionato informático... o) estelionato de subvenção... p) estelionato de apostas esportivas... q) apropriação indébita trabalhista ou previdenciária... r) crimes de falsificação documental... s) bancarrota... t) crimes contra a concorrência... u) crimes de perigo comum... v) corrupção ativa e passiva... 2. do Código Tributário: a) sonegação fiscal… b) contrabando… c) receptação tributária… 3. da lei antidoping... 4. da lei de asilo 5. da lei de migração... 6. da lei de economia externa... 7. Da lei de drogas... 8. da lei de insumos de

Não é nosso escopo tratar dessas soluções. Ante o objetivo de investigar as expectativas constitucionais que recaem sobre os provedores de aplicação de mensageria, necessária a delimitação para fins de concentrar a análise no segundo conjunto referido de medidas, isso é, a obtenção de dados estáticos contidos em suportes eletrônicos, que são justamente as alternativas que pressupõem a colaboração dos provedores na entrega dos dados.

Na categoria dos dados armazenados em suportes eletrônicos, são duas as espécies de dados que mais frequentemente são colocadas à mesa no âmbito do debate do obscurecimento e que nos interessam[39]: (i) os dados armazenados em serviços em nuvem e (ii) os metadados de comunicações[40]. A seleção dessas duas espécies de dados se baseou no teor: (i) das exposições dos expertos na audiência pública realizada no bojo da ADPF 403 e da ADI 5.527; (ii) de relatórios de pesquisa (Abelson et al., 2018, p. 24-26; Berkman Klein Center, 2016); e (iii) de produções científicas especializadas citadas ao longo do texto.

---

drogas... 9. da lei de controle de armas de guerra... 9a. da lei de novos psicotrópicos... 10. do Código de Direito Penal Internacional... 11. da lei de armas...[...]" (Gleizer, Orlandino; Montenegro, Lucas; Viana, Eduardo. O direito de proteção de dados no processo penal e na segurança pública. São Paulo: Marcial Pons, 2021. p. 121 e 124). A Corte di Cassazione italiana apreciou em 2010 um caso em que órgãos de persecução penal lograram êxito em acessar dispositivo eletrônico remotamente com o uso de um software malicioso. Obtido o acesso ao conteúdo dos dados estáticos contidos no dispositivo, os agentes realizaram copia dos dados encontrados. No caso, não ocorreu monitoramento das comunicações em tempo real, razão porque o meio de obtenção de prova empregado foi considerado lícito, pois precedido de autorização judicial e afastada a disciplina da interceptação das comunicações telemáticas. (Pezzotti, Olavo Evangelista. Interceptação telemática, quebra de sigilo de dados e a resistência das big techs: alternativas disponíveis aos órgãos de persecução penal e ao Poder Judiciário. In: Paulino, Galtiênio da Cruz et al. Técnicas avançadas de investigação. Brasília: ESMPU, 2022. p. 271.)

[38] Recentemente o Superior Tribunal de Justiça nulificou prova acessada mediante a operação de "espelhamento" diretamente no computador de autoridades de persecução de uma conta de um investigado usuário do WhatsApp, porquanto se trataria de modalidade híbrida de meio de obtenção de prova. Consignou-se, ainda, a possibilidade de participação do investigador no meio empregado, com poderes de enviar, receber e excluir, o que justificaria a impossibilidade de analogia com o instituto da interceptação telefônica (BRASIL. Superior Tribunal de Justiça. Recurso em Habeas Corpus nº 99.735. Recorrente: A C Da C Recorrente: D C Da C. Relatora Ministra Laurita Vaz. Brasília, 2018. Disponível em: http://www.internetlab.org.br/wp-content/uploads/2018/12/document.pdf. Acesso em: 31 set. 2022).

[39] Descartam-se, com o recorte ora proposto, as técnicas de apreensão física do suporte eletrônico para posterior extração de dados, a exemplo das apreensões realizadas em flagrante delito e mediante mandados de busca, regidas pelo CPP, em seus artigos 6º, II, e 240).

[40] Muito embora tenha relação direta com o objeto da investigação, o acesso a dados e metadados gerados no contexto da Internet das coisas (IoT) também é muito propalado como uma nova abordagem investigativa interessante (Berkman Klein Center, 2016, p. 15; Kuehn, Andreas; Mcconnell, Bruce. Encryption Policy in Democratic Regimes: Finding Convergent Paths and Balanced Solutions. EastWest Institute, 2018. Disponível em: https://www.eastwest.ngo/sites/default/files/ewi-encryption.pdf. Acesso em: 4 out. 2022. p. 24, 40).

# 3 FORMAS ALTERNATIVAS DE INVESTIGAÇÃO COMO RESPOSTA POSSÍVEL AO PROBLEMA DA FALTA DE ACESSO AO CONTEÚDO DAS COMUNICAÇÕES

## 3.1 DADOS EM NUVEM E ANÁLISE DE METADADOS: NOVAS FRONTEIRAS DA PERSECUÇÃO PENAL

Sabe-se que, ao longo da história, a privacidade sempre foi pautada conforme a realidade social, cultural e tecnológica de seu tempo. Da mesma forma, a digitalização dos meios de comunicação impactou fortemente os hábitos da sociedade moderna. A transição das interações até então operadas no mundo analógico para o mundo digital trouxe novas demandas de segurança para o indivíduo, agora sob a rubrica de segurança da informação, seja para as comunicações (dados em trânsito), seja para os dados armazenados. Os sistemas criptográficos são, por isso mesmo, essenciais ao exercício de um plexo de direitos fundamentais, razão pela qual não devem ser enfraquecidos, senão estimulados, mas não a qualquer preço.

Fato é que, em suas duas versões, as guerras criptográficas foram marcadas pela seguinte dicotomia: de um lado, investigadores argumentam que a criptografia inviabiliza seus trabalhos, de outro, especialistas e representantes da indústria e comunidade científica elencam os graves danos que podem advir de iniciativas restritivas da criptografia. Esse antagonismo de visões faz o debate maniqueísta e monocular, desencadeando a perda da noção de profundidade do assunto, que acaba por não refletir questões importantes que estão em jogo, a exemplo de como as autoridades de persecução e repressão de crimes irão se adaptar às novas tecnologias, no caso a criptografia forte, e como as Big Techs podem contribuir com a mitigação dos riscos associados à assimilação da mesma criptografia.

Se é certo que as autoridades de investigação e os sujeitos do processo penal precisarão se adaptar continuamente ao desenvolvimento de novas tecnologias, é igualmente certo que respostas a casos concretos devem ser encontradas dentro do direito vigente, o qual, analisado conglobadamente pode ofertar respostas importantes para questões latentes como estabelecer o que pode ser exigido dos provedores de aplicação de mensageria criptografada em relação ao cumprimento de decisões judiciais que determinem a interceptação telemática ou a quebra de sigilo de dados, em face da essencialidade da criptografia para a concretização de direitos

fundamentais e dos deveres fundamentais dos particulares para com a segurança pública e a administração da justiça.

Táticas e técnicas investigativas deverão necessariamente ser revistas, e a capacitação dos órgãos de Estado é uma etapa imprescindível do percurso da adaptação[41]. Não obstante, o aprimoramento tático e técnico não produz resultado sozinho. A participação das Bigs Techs e dos provedores de aplicação de mensageria criptografada é essencial para que o processo de adaptação se perfectibilize, os quais devem, por força dos deveres fundamentais de cooperar com a segurança pública e com o Poder Judiciário, se desincumbir do ônus de cumprir decisões judiciais, sempre na exata medida do que lhes for técnica (conforme as particularidades do sistema criptográfico e/ou de armazenamento de dados estáticos) e juridicamente exigível. Sem essa dupla conformidade não há que se falar em dever fundamental.

Se é verdade que falta às autoridades de investigação em geral uma visão ampla dos problemas que a restrição da criptografia ocasiona, é igualmente verdade que não lhes haviam sido ofertadas alternativas investigativas até um passado muito recente. A ausência de sinergia é uma característica comum do embate aqui retratado e que precisa, de alguma forma, ser superada. Conforme Carlos Liguori (2022, p. 293-294)[42]:

> A restrição à criptografia é apenas uma saída aparentemente "fácil", que não atinge a raiz do problema. Essa falta de compreensão não está restrita às autoridades de investigação, mas àqueles que se opõem à restrição da criptografia também: sem essa visão ampla, não é possível avançar no debate de forma prescritiva, por mais que os argumentos em prol da criptografia estejam corretos em si. Não se oferecem soluções alternativas às demandas das autoridades, porque, bem, muitas delas também parecem não saber qual é a questão maior que têm de enfrentar (grifo nosso).

[41] Nas palavras de Aranha (2018, p. 13): "Na verdade, o esforço de investigação deva se adaptar às características de plataformas para comunicação segura para exercer o seu papel. Equipar agentes e especialistas com informação técnica acurada sobre essas tecnologias é garantir o poder investigativo do Estado a longo prazo, na medida que tecnologias preservação de privacidade se disseminam cada vez mais. Entretanto, a investigação deve se concentrar em porções da plataforma de comunicação que já estejam acessíveis às autoridades, como a coleta de metadados, infiltração de agentes de polícia em comunidades e grupos de discussão, captura de cópias de segurança armazenadas em serviços de computação em nuvem, entre outros"(grifo nosso).

[42] No mesmo sentido: "[…] devemos pensar agora sobre as responsabilidades das empresas que desenvolvem novas tecnologias e em novas regras e procedimentos operacionais para ajudar as forças policiais e os serviços de inteligência a navegar o emaranhado de questões que certamente acompanharão essas tendências" (Berkman Klein Center, 2016, p. 17, grifos nossos).

Para alterar esse estado de coisas, é indispensável que o direito atue como instrumento de correção das assimetrias de poder, regulando, com parcimônia, as inovações digitais, a partir dos objetivos e dos valores colhidos no próprio ordenamento jurídico, no que os preceitos constitucionais terão destacado papel conciliatório dos interesses em jogo. A preocupação em compatibilizar as inovações com os princípios concretizados na Constituição parece caminhar no sentido da construção de uma autêntica "responsabilidade pela inovação" (Hoffmann-Riem, 2022, p. 72). O ordenamento jurídico deve albergar não apenas o direito ao exercício da liberdade, como também a salvaguarda contra as consequências do uso da liberdade por outros, o que engloba a garantia de proteção contra as consequências danosas para a coletividade do uso das liberdades individuais (Hoffmann-Riem, 2022, p. 96).

## 3.2 SERVIÇOS DE NUVENS, BACKUP E ARMAZENAMENTO DE DADOS – VANTAGENS E DESVANTAGENS

Entende-se por backup a atividade de produzir cópias de segurança dos dados digitais (fotos, vídeos, documentos, software, entre outros) que repousam em determinado dispositivo eletrônico, com a finalidade de restaurá-los, em caso de perda acidental de arquivos ou falha do sistema físico que lhes dá suporte. Tais cópias podem ser armazenadas em um sistema de backup em nuvem ou em outro dispositivo físico do qual disponha o titular desses dados.

Se num passado não tão distante os backups de dados eram feitos predominantemente em meios materiais, como mídias óticas, magnéticas etc. (disquetes, CDs, DVDs, pen-drives e HDs externos), que poderiam se perder, deteriorar, apresentar falhas ou dificuldades de compatibilidade com tecnologias posteriores, ou simplesmente serem infectados por algum malware, hoje o panorama se alterou drasticamente com a ascensão e consolidação dos serviços de nuvens ofertados por grandes companhias tecnológicas.

Implementada em meados dos anos 2000, a computação em nuvem ainda é uma tecnologia relativamente nova. Dentre os maiores provedores, estão o Google Drive (mais de 800 milhões de usuários inscritos), o iCloud, da Apple (contando com mais de 780 milhões de usuários), e o Dropbox (supera os 600 milhões de usuários ao redor do globo) (Liguori, 2022, p. 225).

Grosso modo, a realização de um backup em nuvem pode ser sintetizada como a ação de transferir arquivos digitais contidos em dispositivos eletrônicos para servidores externos (data centers), normalmente operados por grandes corporações tecnológicas, como Apple, Google e Amazon, que espalham suas infraestruturas por distintos lugares.

Os serviços de armazenamento em nuvem equivalem a verdadeiros “discos rígidos on-line”, com limites de armazenamento de acordo com eventual plano selecionado, bastando, para acesso ao conteúdo armazenado, que se disponha de um computador conectado à internet e das credenciais de acesso.

Em suma, aquele que adere aos serviços de nuvem obtém não só a ampliação da disponibilidade dos seus dados (que agora podem ser acessados de qualquer lugar, inclusive pelo smartphone), como também economiza espaço de armazenamento de arquivos em seus dispositivos, além, é claro, de poder contar com a função que parece, a nosso juízo, ser a mais interessante de todas, a realização do backup dos dados digitais. Acresça-se que o uso da computação em nuvem se faz presente em diversas tarefas comuns, tais como no envio e recebimento de correios eletrônicos, na publicação de imagens e comentários em redes sociais e no desenvolvimento de trabalhos por meio de aplicações de edição de texto que podem ser compartilhadas entre colegas. Pode-se dizer que os serviços de nuvem representam “[...] uma camada conceitual que abstrai toda infraestrutura da plataforma computacional, deixando os serviços transparentes ao usuário que é atendido como se os dados e programas estivessem em sua máquina local” (2022, p. 4). Segundo Pedrosa e Nogueira (2011, p. 4):

> Os benefícios obtidos com esta tecnologia tem [sic] sido expressivos, tanto para grandes corporações, com um grande apelo econômico além da flexibilidade e dinamicidade proporcionada, quanto para o usuário comum, que usufrui principalmente da mobilidade, integração e inteligência das aplicações. A atual estrutura das nuvens tem se mostrado robusta e confiável no sentido de garantir ao usuário uma boa qualidade e quantidade de aplicações e serviços.

Como visto, a maior parte dos problemas que envolvem a regulação da criptografia se deve à inviabilidade técnica de interceptação dos dados em fluxo em formato legível, por conta da criptografia ponta a ponta, e dos dados estáticos em dispositivos com proteção por criptografia forte. Não obstante isso, a crescente oferta e aceitação dos serviços de nuvem por usuários comuns e empresas abre importante via investigativa, que é a obtenção dos dados

que repousam nesses ambientes, aí incluídos os backups de conversas em aplicativos de mensageria.

A vantagem mais evidente é que os dados repousam, como regra, em formato legível nos serviços de nuvem. Nessas plataformas, tanto o fluxo como o armazenamento de dados são criptografados, mas, na maior parte das vezes, os provedores guardam cópia da chave criptográfica, o que permite o acesso e o processamento de dados do usuário (Berkman, 2016, p. 11). Liguori (2022, p. 228-229) elenca os três principais motivos para que isso ocorra:

> Em primeiro lugar, garante-se alguns benefícios aos usuários, como a possibilidade de recuperação das chaves, caso eles esqueçam seu login e senha ou tenham suas contas invadidas por terceiros. Não havendo a guarda da cópia das chaves, o conteúdo se perderia [...]. Além disso, o acesso e processamento dos dados pelo sistema são necessários para oferecer ao usuário mecanismos de indexação e busca de dados em suas plataformas [...]. Em segundo lugar, o acesso aos dados na forma legível é necessário para garantir a segurança e a estabilidade dos servidores da nuvem, além de certificar que os materiais lá armazenados são lícitos. [...] Por fim, em terceiro lugar, o próprio modelo de negócio das plataformas de serviços em nuvem gera desincentivos à implementação de mecanismos que as impeçam de acessar os conteúdos nelas armazenados. Principalmente no caso de plataformas que o fornecem de forma gratuita, o acesso aos dados é essencial para monetização do serviço: o tratamento dos dados dos usuários é realizado para o direcionamento de propagandas.

Tomando o iCloud, da Apple, como ilustração, pode-se notar que muito embora a empresa afirme utilizar criptografia de ponta a ponta nas comunicações travadas em suas aplicações, sabe-se que a criptografia não é linear em todos os seus produtos e serviços. O serviço de backup do iCloud, por exemplo, é responsável por viabilizar a recuperação de dados diretamente nos servidores da empresa. A despeito de criptografar os backups, a companhia guarda consigo cópia das chaves no sentido de salvaguardar que aqueles usuários que perderam seus dados não fiquem deles despojados permanentemente em caso de perda ou esquecimento da senha de acesso. Logo, em que pese o dados contidos no backup estejam resguardados de investidas maliciosas externas pela criptografia, eles sempre poderão ser acessados pela Apple[43] e, já que a companhia retém para si cópia das chaves criptográficas, pode ser forçada judicialmente a entregar os dados armazenados no iCloud.

[43] Na própria descrição da metodologia de segurança de dados, a Apple deixa claro que "O iCloud protege suas informações criptografando-as quando estão em trânsito, armazenando-as em um formato criptografado e protegendo as chaves de criptografia nos centros de dados da Apple. Os centros de dados da Apple e de terceiros podem ser usados para armazenar e processar dados. Ao processar dados armazenados em um centro de dados de terceiros, as chaves de criptografia serão acessadas apenas pelo software da Apple em execução em servidores seguros e apenas durante a execução do processamento necessário" (Disponível em: https://support.apple.com/pt-br/HT202303.
Acesso em: 4 dez. 2022. Grifo nosso).

Acresça-se que vários serviços de nuvem apresentam a funcionalidade como backup em tempo real[44] e o automático[45], tornando desnecessário que sejam programados backups periódicos. Ademais, é comum que os desenvolvedores de sistemas operacionais disponibilizem serviços gratuitos de nuvem associados aos seus produtos: os dispositivos da Apple, por exemplo, vêm acompanhados do iCloud, o Google Drive é disponibilizado nos dispositivos operados pelo sistema Android e OneDrive é a opção para o Windows, da Microsoft. Embora seja incorreto afirmar que os serviços de nuvem venham habilitados por padrão nesses sistemas, já que demandam inscrição e ativação pelo usuário, nota-se que há muito mais do que somente um forte apelo ao seu uso; a integração do usuário a esses serviços não apenas faz parte do modelo de negócio dessas Big Techs, como é essencial a algumas das funcionalidades mais interessantes dos sistemas operacionais,[46] a exemplo da sincronização de dados em todos os dispositivos de um usuário.

Embora não tenha sido citado, na audiência pública da ADPF 403 e ADI 5.527, o acesso aos backups armazenados em nuvem é defendido como importante alternativa investigativa em diversos trabalhos[47], a ponto de se tornar comum deparar com assertivas no sentido de que "[...] dados também podem ser vazados em meios não encriptados, através de backups na nuvem e sincronização em vários dispositivos" (Berkman Klein Center, 2016, p. 11).

Não obstante a obtenção do conteúdo de diálogos em nuvem desponte como relevante alternativa investigativa, é certo que o emprego de novas arquiteturas tecnológicas vem suscitando, como é comum, importantes problemas jurídicos; e a coleta de dados localizados no exterior parece ser, no momento, o principal deles.

Uma das características das arquiteturas dos serviços de nuvem é a fragmentação das contas dos usuários e a distribuição do conteúdo de comunicação, metadados e dados pessoais entre

---

[44] Tão logo um arquivo é criado ou é salvo no dispositivo, uma cópia é salva na nuvem.

[45] No iCloud, como exemplo, pode ser que o usuário do serviço mantenha ativa a função de realização do backup automático, o que significa que será realizada uma cópia de segurança dos dados do dispositivo toda vez que ele estiver ligado à alimentação, bloqueado e conectado à internet.

[46] Conforme: https://www.computerworld.com/article/2476176/mac-os-x-how-to-avoid-paying-applefor-extra-icloud-storage.html. Acesso em: 4 de dez. 2022. No mesmo sentido: https://www.computerworld.com/article/2882210/warning-apple-wants-to-get-you-hooked-onicloud.html. Acesso em: 4 de dez. 2022.

[47] Dentre outros: National Academies of Sciences, Engineering & Medicine, 2018, p. 71; Kuehn; Mcconnell, 2018, p. 32; Gill; Israel; Parsons, 2018, p. 14; Berkman Klein Center, 2016, p. 12-14. Liguori, 2022, p. 227-228. Aranha, 2018, p. 13.

os diversos data centers[48], muitas vezes distribuídos geograficamente em diferentes partes do globo, com o escopo de reduzir a latência da rede e fornecer um serviço de alta qualidade. Seja por questões relacionadas ao modelo de negócio ou por razões de estratégia técnica[49], a distribuição da infraestrutura por distintos lugares, por vezes englobando a jurisdição de mais de um país, desborda em inevitável internacionalização de dados, daí emergindo questionamentos acerca do poder de autoridades nacionais de obter, com base exclusivamente nas normas processuais internas, dados armazenados fora do território do país onde o fato é investigado ou processado (Valverde, 218).

> Outrossim, outro efeito prático do recrudescimento da criptografia forte foi a consequente elevação do volume de requisições judiciais objetivando o acesso a dados digitais sigilosos armazenados além do espaço territorial da jurisdição interessada a atrair uma sempre crescente atenção de todos os atores envolvidos em tais demandas, dadas as repercussões para os negócios do setor. (Swire, Hemmings; Vergnollie, 2016)

No Brasil, a Ação Declaratória de Constitucionalidade nº 51 (Brasil, 2022) vem centralizando o debate acerca da obtenção de dados armazenados por provedores de aplicação de serviços de nuvem. Ajuizada pela Assespro Nacional (Federação das Associações das Empresas Brasileiras de Tecnologia da Informação), a ADC tem por objetivo, em linhas gerais, a declaração de validade do uso das cartas rogatórias (artigos 780[236] e 783[237] do CPP e artigo 237, II[50], do CPC) e do Acordo de Assistência Judiciária Mútua (MLAT - Mutual Legal Assistance Treaty) firmado entre Estados Unidos e Brasil (assimilado pelo ordenamento nacional por meio do Decreto nº 3.810, de 2 de maio de 2001[51]) como instrumento jurídico

---

[48] Data center pode ser conceituado como extenso e complexo sistema de hardware e software necessário ao funcionamento da computação em nuvem, ou seja, à entrega de aplicações de internet ao usuário como um serviço. Dos atuais 23 (vinte e três) data centers da companhia norte-americana Google LLC, 8 estão localizados fora dos Estados Unidos por exemplo: um na América do Sul (Chile) 06 (seis) na Europa e 2 (dois) na Asia. (conforme: https://www.google.com/about/datacenters/locations/. Acesso em: 3 jan. 2023.

[49] "A necessidade de as próprias empresas armazenarem essa grande quantidade de informações por questões internas gerenciais, ou por determinação das legislações às quais se consideram submetidas, resultou em que o armazenamento de dados ocorresse em servidores nos mais diversos países, seguindo critérios econômicos e fiscais. Também, por razões de segurança, há servidores replicados em locais diferentes do globo e informações que são armazenadas de forma fracionada" (Domingos; Röder, 2017, p. 33).

[50] "Art. 237. Será expedida carta: [...] II - rogatória, para que órgão jurisdicional estrangeiro pratique ato de cooperação jurídica internacional, relativo a processo em curso perante órgão jurisdicional brasileiro" (BRASIL, 2015).

[51] "Artigo I - Alcance da Assistência. 1. As Partes se obrigam a prestar assistência mútua, nos termos do presente Acordo, em matéria de investigação, inquérito, ação penal, prevenção de crimes e processos relacionados a delitos de natureza criminal. 2. A assistência incluirá: a) tomada de depoimentos ou declarações de pessoas; b) fornecimento de documentos, registros e bens; c) localização ou identificação de pessoas (físicas ou jurídicas) ou bens; d) entrega de documentos; e) transferência de pessoas sob custódia para prestar depoimento ou outros fins;

único destinado à obtenção de dados digitais localizados fora do Brasil para fins de persecução penal. Acaso seja acolhida a pretensão, seria inviável a concretização de requisições judiciais diretas destinadas aos provedores de serviços de nuvem, tal como possibilitado pelo artigo 11[52240] do Marco Civil da Internet e pelo artigo 18[53] da Convenção de Budapeste[242] sobre Cibercriminalidade (incorporada ao nosso ordenamento jurídico recentemente [54] , por meio do Decreto Legislativo nº 37, em dezembro de 2021). Objetivamente, busca-se estabelecer na ADC 51 qual é a via constitucionalmente adequada para a obtenção de dados digitais armazenados em data centers fora do território brasileiro: se é via cooperação jurídica internacional (MLAT) ou via sistema de requisição direta destinada aos provedores de aplicação de nuvem positivado (Marco Civil da Internet combinado com a Convenção de Budapeste).

---

f) execução de pedidos de busca e apreensão; [...] Artigo II - Autoridades Centrais. 1. Cada Parte designará uma Autoridade Central para enviar e receber solicitações em observância ao presente Acordo. 2. Para a República Federativa do Brasil, a Autoridade Central será o Ministério da Justiça. No caso dos Estados Unidos da América, a Autoridade Central será o Procurador-Geral ou pessoa por ele designada. 3. As Autoridades Centrais se comunicarão diretamente para as finalidades estipuladas neste Acordo. [...] Artigo IV - Forma e Conteúdo das Solicitações. 1. A solicitação de assistência deverá ser feita por escrito, a menos que a Autoridade Central do Estado Requerido acate solicitação sob outra forma, em situações de urgência. Nesse caso, se a solicitação não tiver sido feita por escrito, deverá ser a mesma confirmada, por escrito, no prazo de trinta dias, a menos que a Autoridade Central do Estado Requerido concorde.

[52] "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 e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. § 1º O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil. § 2º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil. § 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações" (Brasil, 2014).

[53] Artigo 18º. – Injunção 1. Cada Parte adotara as medidas legislativas e outras que se revelem necessarias para habilitar as suas autoridades competentes para ordenar: a. A uma pessoa que se encontre no seu território que comunique os dados informaticos especificos, na sua posse ou sob o seu controle e armazenados num sistema informatico ou num outro suporte de armazenamento de dados informaticos; e b. A um fornecedor de serviços que preste serviços no território da Parte, que comunique os dados na sua posse ou sob o seu controle, relativos aos assinantes e respeitantes a esses servicos. (Brasil. Decreto Legislativo nº 37 de dezembro de 2021. Aprova o texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001. Brasília, 2001. Disponível em: https://legis.senado.leg.br/norma/35289207/publicacao/35300588. Acesso em: 25 dez. 2022. [242] BRASIL. Senado Federal. Projeto de decreto legislativo n° 255, de 2021. Aprova o texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001. Diário do Senado Federal. Brasília, DF. 14 out. 2021. Disponível em: https://legis.senado.leg.br/diarios/ver/108151?sequencia=129. Acesso em 26 dez. 2022.

[54] A relevância da adesão do Brasil à Convenção de Budapeste é incontestável. O instrumento internacional já foi subscrito por mais de 60 Estados, servindo de base para a construção de legislações.

O julgamento da ADC 51 ainda se encontra pendente de conclusão[55], todavia o Ministro Gilmar Mendes, relator da ação, teceu relevantes considerações em seu voto, proferido em 29 de setembro de 2022, que possivelmente servirão de norte para as discussões em torno do assunto (Brasil, 2022): (i) pontuou que, depois das revelações do escândalo Snowden, passou-se a perceber uma forte tendência de Estados nacionais criarem leis internas submetendo entidades com atuação na internet ao dever de cumprimento de ordens judiciais, mesmo que partes das operações de tratamento e armazenamento de dados não aconteçam totalmente do país (trata-se do fenômeno denominado "territorialização" do ciberespaço); (ii) firmou que o mote principal dessa "territorialização" do ciberespaço, a exemplo do que se dá com o art. 11 do Marco Civil da Internet, é o de salvaguardar a soberania do país ao obrigar que certos tipos de dados coletados no Brasil sejam aqui armazenados e processados; (iii) consignou que a necessidade do pedido diplomático com respectiva resposta da jurisdição detentora do controle sobre os dados, aliada às demais formalidades do mecanismo MLAT, torna a cooperação internacional inatamente morosa, afora o "[...] baixo índice de efetividade desses pedidos de assistência jurídica enviados aos Estados Unidos para a quebra de sigilo de dados ou obtenção de informações telemáticas", algo em torno de apenas 22,5% dos casos com respostas positivas; (iv) ponderou que o firmamento de acordos internacionais unilaterais ou multilaterais e a expedição de cartas rogatórias se notabilizaram historicamente como instrumentos aceitos para a obtenção de bens corpóreos situados no exterior, dada a excepcionalidade dessas medidas e diante da precisa delimitação das fronteiras territoriais, lógica esta inaplicável aos dados digitais; (v) acrescentou que os embates entre autoridades de persecução e empresas de tecnologia estão relacionados à natureza diferenciada e a-territorial (Daskal, 2015) (em razão da infantilidade decorrente do formato em bits) dos dados digitais como meios de prova, porquanto as particularidades técnicas do armazenamento em sistemas de nuvem[56] tornariam inadequado o critério territorial de delimitação da abrangência da jurisdição estatal; (vi) observou que o art. 11 do Marco Civil da Internet está em consonância com o art. 18 da Convenção de Budapeste, e ambos são norma especiais em relação ao regramento próprio das formas de cooperação jurídica internacional (MLAT e cartas rogatórias); (vii) concluiu pela constitucionalidade tanto do modelo do MLAT como do sistema de requisição direta, sendo aquele complementar a este. Por fim, o Ministro Gilmar

[55] Os Ministros André Mendonça e Nunes Marques votaram pelo não conhecimento das ações e, no mérito, acompanharam os termos do voto do relator. Na sequência da votação, o Ministro Alexandre de Moraes pediu vista e o julgamento foi suspenso.

[56] Tais como mobilidade, divisibilidade dos dados, fragmentação dos dados por diversos data centers e possibilidade de dissociação entre o local do acesso e a localização do dado digital, entre outras.

Mendes consignou que eventual decisão adotada pelo STF no bojo da ADC 51 deve ser levada ao conhecimento dos Poderes Executivo e Legislativo da União para que promovam as medidas necessárias.

> [...] ao aperfeiçoamento do quadro legislativo, com a discussão e a aprovação do projeto da Lei Geral de Proteção de Dados para Fins Penais (LGPD Penal) e de novos acordos bilaterais ou multilaterais para a obtenção de dados e comunicações eletrônicas, como, por exemplo, a celebração do Acordo Executivo definido a partir do Cloud Act (Brasil, 2022)[57].

Seja como for, em sendo o mérito da ação declaratória enfrentado, produzir-se-ão importantes efeitos nas investigações e processos vindouros e em curso, muitos dos quais paralisados por negativas de cooperação de provedores de aplicação em casos de requisições diretas por autoridades brasileiras, colocando fim à controvérsia que há muito se faz presente nos tribunais nacionais.[58]

Também na ADC 51 foi realizada audiência pública (Brasil, 2020) para melhor compreensão das inúmeras questões técnicas e problemas jurídicos que orbitam o acesso extraterritorial de dados para uso no processo penal[59].

Conquanto todo o imbróglio jurídico em torno do acesso a evidências extraterritoriais armazenadas desafie o significado de conceitos tradicionais, como jurisdição, soberania e territorialidade penal (nos ambientes virtuais), não se pode perder de vista que, até que sobrevenha solução definitiva para a controvérsia, todos os dispositivos legais e internacionais

---

[57] Lei aprovada pelo Congresso dos Estados Unidos, em março de 2018, muito motivada pelas intensas disputas judiciais em que o FBI pretendia obter acesso a dados em poder da Microsoft que estavam armazenados em servidores situados na Irlanda. A lei permite, em termos gerais, que os EUA firmem acordos executivos (em vez de tratados) com países que atendam a várias exigências, tudo com vistas a possibilitar a cooperação direta com Estados signatários, facilitando o fluxo dessa relação. Para mais informações sobre o tema, ver: Veronese, Alexandre; Calabrich, Bruno. Crimes na internet e o Brasil no cenário da cooperação jurídica internacional. Portal Jota, 24 abr. 2021. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/judiciario-e-sociedade/crimes-nainternet-e-o-brasil-no-cenario-de-cooperacao-juridica-internacional-24042021. Acesso em: 10 dez. 2022; Valverde, 2018.

[58] No Inquérito nº 784, de 2013, o Google se insurgiu, via mandado de segurança, contra ofício requisitório expedido pela Polícia Federal, objetivando quebra de sigilo de contas de usuários do Gmail, ao argumento de que estaria impedido de fornecer os dados eletrônicos fora do sistema de cooperação internacional. Em 2015, foi a vez da Microsoft negar cumprimento de ordem judicial de quebra de sigilo de e-mails do Hotmail pelos mesmos argumentos utilizados pelo Google (cf. Recurso em Mandado de Segurança nº 46.685/MT. Min. rel. Leopoldo de Arruda Raposo, julg. 26.03.2015). Em ambos os casos, as decisões foram contrárias aos interesses dos provedores de correio eletrônico. Em 2014, o Yahoo! foi acionado pelo Ministério Público Federal em ação pública que tinha como fundamento o descumprimento reiterado de ordens judiciais de entrega de dados de seus usuários (os exemplos são muitos).

[59] A transcrição da referida audiência pública está disponível em: https://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADC51Transcricoes.pdf.

criados ou incorporados ao ordenamento jurídico interno continuam a gozar de presunção de constitucionalidade das leis, inexistindo qualquer determinação que restrinja sua produção de efeitos até o presente momento.[60]

Outro ponto que merece atenção das autoridades de persecução é a possível modificação de alguns serviços de nuvem que possam tornar inviável o acesso ao conteúdo em formato legível. Para tanto, basta que a criptografia seja implementada sem a guarda de chaves, a exemplo do que já ocorre com alguns provedores menos notórios, como o Mega. Esta pode ser uma tendência de resposta dos provedores às recentes legislações de proteção de dados, que estabelecem rigorosas penalidades e obrigações na ocorrência de incidentes de segurança de dados, como se nota da leitura dos artigos 42 a 49 e 52 da LGPD, dentre outros. O próprio Whatsapp já contempla a opção de backup criptografado sem a guarda de chaves, embora a função não venha habilitada por padrão após a instalação.

## 3.3 METADADOS – VANTAGENS E DESVANTAGENS

É inegável que assimilação da criptografia forte em aplicativos de mensageria provocou e provoca impactos concretos à atividade persecutória do Estado em relação aos crimes praticados por meio da internet, a exemplo da mercancia de drogas, da promoção da pornografia infantil, de crimes que se utilizam do anonimato (como fraudes mediante uso perfil falso, v.g), dos crimes de ódio, da cooptação sexual de crianças e adolescentes, ou mesmo a articulação de movimentos terroristas e contra a ordem democrática.

Contudo, há equívoco na afirmação genérica de que a criptografia simplesmente inviabiliza investigações.

Sabe-se que as investigações criminais são verdadeiros quebra-cabeças destinados à descoberta da materialidade e autoria delitiva, o que se dá por meio do levantamento e apuração de uma série de evidências que se conectam com o crime e suas circunstâncias ou com as pessoas nele envolvidas. Mesmos nos crimes praticados por meio da internet, não é

[60] Com efeito, dado este quadro, é possível que se tomem por ilícitas as recusas de entrega de dados pelos provedores de serviços de nuvens que privilegiam o caminho da cooperação internacional em prejuízo da via da requisição direta.

raro que a empreitada criminosa se desenvolva por mais de uma via de atuação, sendo que ação do agente fatalmente deixará para trás rastros físicos ou digitais.

A popularização do acesso a dispositivos eletrônicos móveis como tablets, smartphones e smartwatch são um importante elemento propulsor do crescimento da quantidade total de dados gerados no mundo. Trajetos e rotas desenvolvidas por veículos privados ou públicos são registrados, assim como são recolhidos a todo momento os dados sobre localização de usuários, além da coleta de opiniões em redes sociais, de dados de saúde e de metadados de comunicações digitais, tais como e-mails[61], mensagens instantâneas trocadas em aplicativos de mensageria, que podem incluir texto ou arquivos variados (imagens, áudio, vídeos, dentre outros conteúdos) (Correa, 2018).[62]

Os metadados (também denominados metainformações ou metadados descritivos) são recorrentemente designados como dados que descrevem outros dados, isto é, são dados sobre dados; são detalhamentos que integraram a estrutura do dado principal, fazendo deste um conglomerado informações uteis. Simplificadamente, os metadados são “marcos ou pontos de referência que permitem circunscrever a informação sob todas as formas”[63], ou seja, são uma síntese de informações sobre o conteúdo, forma ou processos de uma determinada fonte. São dados estruturados sobre qualquer coisa que possa ser nomeada, como sítios da Web, músicas, imagens, livros, artigos científicos, processos, produtos, dados de pesquisa, pessoas (e suas atividades), conceitos e serviços.[64]

---

[61] No caso de uma troca de e-mail entre dois interlocutores, o conteúdo é o assunto e o corpo do e-mail, não contemplando as informações "de" e "para", que identificam remetente e destinatário e seriam os metadados da comunicação. Numa correspondência epistolar, eventuais informações inseridas no corpo externo do envelope seriam metadados da comunicação.
lo”.

[62] Não é exagerado observar que, em verdade, a maioria dos aplicativos dominantes são, a um só tempo, gratuitos e providos de arquitetura voltada a coletar o maior volume possível de dados dos seus usuários. O motivo do arranjo é singelo: “o usuário é o produto que está sendo vendido para anunciantes”. (Belli, Luca; Zingales, Nicolo. Novas Regras do WhatsApp: a proteção de dados se torna um luxo para 2 bilhões de pessoas? 2021. Disponível em: https://mittechreview.com.br/novas-regras-de-facebook-e-whatsapp-a-protecao-de-dados-se-tornaum-luxo-para-2-bilhoes-de-pessoas/. Acesso em: 11 dez. 2022.)

[63] O que são Metadados? Metadados, [s.d.]. Disponível em: http://www.metadados.pt/oquesaometadados/. Acesso em: 11 dez. 2022.

[64] Noções básicas de metadados. Dublincore [s.d.]. Disponível em: https://www.dublincore.org/resources/metadata-basics/ Acesso em: 08 jan. 2023

O prefixo “meta” vem do grego e significa “além de”[65], de modo que os metadados são elementos que possibilitam uma compreensão que vai além do núcleo do dado em si, abrangendo informações uteis à sua organização, pesquisa e classificação. Logo, os metadados são informações que “permitem a indexação, a classificação, ou mesmo a investigação do próprio conteúdo do dado sem que seja necessário acessá-

Por meio dos metadados é possível extrair e consolidar dados de várias fontes distintas numa base de dados que possa ser servir à consulta integrada pelos interessados.

No âmbito da União, o Decreto 10.278 de 2020 regulamenta dispositivos das Leis Federais 13.874/2019 (Lei de Liberdade Econômica) e 12.682/12 (que trata da elaboração e o arquivamento de documentos em meios eletromagnéticos), para estabelecer a técnica e os requisitos para a digitalização de documentos públicos ou privados, a fim de que os documentos digitalizados produzam os mesmos efeitos legais dos documentos originais. Em seu artigo 3º, inciso II, o decreto define metadados como dados estruturados que permitem classificar, descrever e gerenciar documentos, prevendo, ainda, que o armazenamento de documentos digitalizados assegurará a indexação de metadados que possibilitem a localização e o gerenciamento do documento digitalizado, bem como a conferência do processo de digitalização adotado (Brasil, 2012).

Quando digitais, os metadados[66] são todas as informações descritivas sobre dados digitais ou ações em ambiente digital que não se refiram ao seu conteúdo. Com efeito, metadado digital é o “[...] dado que descreve atributos de um recurso, caracteriza suas relações, apoia sua descoberta e uso efetivo, e existe em um ambiente eletrônico.

Usualmente consiste em um conjunto de elementos, cada qual descrevendo um atributo do recurso, seu gerenciamento, ou uso” (Campos, 2007, p. 19).

[65] Noções básicas de metadados. Dublincore [s.d.]. Disponível em: https://www.dublincore.org/resources/metadata-basics/ Acesso em: 08 jan. 2023

[66] Para aprofundamentos sobre o tema metadados digitais ver: Campos, Luiz Fernando de Barros. Metadados digitais: revisão bibliográfica da evolução e tendências por meio de categorias funcionais. Encontros Bibli: revista eletrônica de biblioteconomia e ciência da informação, [S. l.], v. 12, n. 23, p. 16–46, 2007. DOI: 10.5007/1518-2924.2007v12n23p16. Disponível em: https://periodicos.ufsc.br/index.php/eb/article/view/1518-2924.2007v12n23p16. Acesso em: 01 jan. 2023.

Acerca dos metadados gerados nas comunicações digitais, Abreu e Antonialli (2017, p. 19) ensinam que:

> [...] consideram-se metadados todos os dados e registros gerados a partir de uma comunicação e que não constituam o seu conteúdo em si, como, por exemplo, data, hora e duração da comunicação, remetente, destinatários, eventuais dados de localização geográfica do dispositivo (como Estação Rádio Base), códigos de identificação de dispositivos (como IMEI) etc.

No âmbito das comunicações digitais, a quantidade de metadados gerados é muito maior[67][265] do que a verificada nas comunicações telefônicas. Basta que se pense que no universo digital os metadados não se limitam aos dados sobre comunicações entre usuários conectados à internet; incluem também informações sobre arquivos armazenados e seu compartilhamento[68] com terceiros, registros de conexões e dispositivos eletrônicos, registro de ações e interações em aplicações[69] e até mesmo informações cadastrais do usuário de aplicação, tais como login, nome, data de nascimento, entre outros, a depender dos requisitos para cada serviço.

Via de regra, a criptografia não protege os metadados gerados nas comunicações digitais, os quais ficam disponíveis e legíveis, mantidos em texto simples e não formatado. Assim ocorre

---

[67] Sobre a exploração de metadados para promoção da vigilância em redes sociais, vide: GRESCHBACH, Benjamin; KREITZ, Gunnar; BUCHEGGER, Sonja. The devil is in the metadata— New privacy challenges in Decentralised Online Social Networks. In:Pervasive Computing and Communications Workshops (PERCOM Workshops), 2012, Lugano. p. 333-339. Disponível em: https://ieeexplore.ieee.org/document/6197506. Acesso em: 16 abr. 2022.

[68] São exemplos dessas informações: o tipo de arquivo (texto, foto ou vídeo), a extensão do arquivo (.jpg, .png, .mp4, .mkv, etc.), o tamanho do arquivo, quando o arquivo foi criado, quais usuários possuem privilégios de administrador, dentre outros. Um padrão de formato de arquivos de imagens e áudios merece destaque, o EXIF (Exchangeable Image File Format). Presente em câmeras digitais e smartphones, o EXIF é um mecanismo técnico que possibilita que se registrem, no próprio arquivo da imagem, informações sobre as condições técnicas do momento da captura, como um metadado. Em cada imagem, a câmera irá registrar, automaticamente, informações como marca e modelo da câmera, tipo de exposição, zoom, ISO, número de pixels, hora, data e, quando disponíveis, dados de geolocalização (coordenadas de GPS) de onde foi realizado o registro. Note-se, ademais, que metadados são informações adicionais que não aparecem exclusivamente em imagens e fotos, estando presentes também em arquivos digitais das mais variadas extensões, do que ressai o enorme potencial de benefício para investigações. Nesse sentido: Cossetti, Melissa Cruz. O que são dados EXIF de fotos: em cada foto, a câmera ou o celular gera e registra dados exif sobre como, quando e onde a imagem foi registrada. Em cada foto, a câmera ou o celular gera e registra dados EXIF sobre como, quando e onde a imagem foi registrada. 2019. Disponível em: https://tecnoblog.net/responde/oque-sao-dados-exif-de-fotos-e-como-encontra-los-ou-esconde-los/. Acesso em: 04 out. 2022, e Barreto, Alesandro Gonçalves; Caselli, Guilherme. Exif Metadata - A investigação policial subsidiada por sua extração e análise. 2016. Disponível em: https://delegados.com.br/noticia/exifmetadata-a-investigacao-policial-subsidiada-por-sua-extracao-e-analise. Acesso em: 04 out. 2022. [267] Na dicção legal registro de conexão é "[...] o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados" – Art. 5º, VI, MCI).

[69] Aqui estão incluídos os "logs de conexão", que são "[...] o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dado", de acordo com o Marco Civil da Internet.

em razão da importância dos metadados ao funcionamento dos próprios sistemas de diversas aplicações em geral[70] e por razões inerentes aos modelos de negócios de algumas empresas.

Apesar de os metadados não revelarem o conteúdo das comunicações digitais protegidas pela criptografia, eles podem fornecer informações que vão muito além disso. Podem revelar: a rede de comunicação do indivíduo, não se limitando àqueles com quem o interlocutor se comunica diretamente, mas também os seus contatos mais frequentes; a localização aproximada dos comunicantes; a quantidade e a natureza dos dados (texto, vídeos, imagens e áudios) trocados, a data e a hora da troca. Além disso, ao localizar as antenas transmissoras, será possível identificar o posicionamento dos telefones dos integrantes de um grupo de pessoas, o que poderá determinar onde, em que ocasiões e com qual frequência os seus membros se reúnem, permitindo que a polícia realize operações para cessar práticas delitivas, localizar e prender suspeitos ou angariar provas. Por meio dos metadados de comunicação digital é possível especificar fluxos de dados trocados entre indivíduos e em grupos, pesquisas e assuntos de interesse na Internet, sem mencionar na possibilidade de infiltração de agentes policiais em grupos de mensagens de organizações criminosas.

É consabido que organizações criminosas se preocupam com o encobrimento dos rastros de seus negócios, inclusive pelo uso de aplicativos de mensageria com criptografia forte. É inegável, no entanto, o potencial de uma boa exploração de metadados para as atividades de investigação. Com o tratamento e a consequente análise de conteúdo, os metadados podem colaborar na recomposição histórica de crimes, constituindo evidências que sirvam para refutar ou confirmar álibis, para justificar ações ou refutar versões. Como observa Rafael Lima Linhares, o tratamento e análise de metadados vem sendo uma alternativa que traz bons resultados, notadamente quando as autoridades de investigação possuem "[...] o sacramento de seguir escopos definidos, e sua agência o costume de palmilhar sobre bancos tipológicos, sedimentados em algoritmos próprios, criados com base em conhecimentos de background, ou seja, de investigações passadas e aprendidas (Linhares, 2022, p. 177).

[70] Conforme Gill, Israel e Parsons (2018, p. 85): "For example, in 2014 Facebook's former Chief Security Officer admitted the company "has been able to deploy end-to-end encryption for a long time" but avoided doing so citing of concerns about usability and complexity. These variables, taken together, mean that we are unlikely to see a digital ecosystem where all (or even most) data held by intermediaries is both encrypted and unavailable to those intermediaries by default, at least for the foreseeable future." [270] GILL, Lex; Israel, Tamir; Parsons, Christopher. Shining a Light on the Encryption Debate: a Canadian field guide. CitizenLab, e Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic., 2018. p. 04 [271] Corrêa, 2018, p. 268.

No caso do WhatsApp, a sua política de privacidade[71] elenca os dados que são coletados automaticamente: dados fornecidos diretamente pelos usuários por ocasião do registro na aplicação ou resultantes do seu uso[72]; dados coletados com terceiros

(contatos, v.g); dados retidos por serviços integrados ao aplicativo e; dados coletados das empresas parceiras do WhatsApp ou da Meta. Ou seja, praticamente tudo que não for conteúdo da uma troca de mensagens poderá ser armazenado pela aplicação, desde que compatível com a política de privacidade e com os termos de uso. Consequentemente, mediante ordem judicial válida, diversos dados poderão ser fornecidos para subsidiar investigações e produções probatórias como, por exemplo: (i) dados básicos de registro de contas e histórico de informações dos SIM cards; (ii) informações sobre uso e conexão do Whatsapp Web, bem como hora e a data da última conexão; (iii) logs (registros) de acesso, aí incluído os protocolos de internet (IPs) do registro inicial e de conexão dentro de um período delimitado, com especificações de data, horário e a porta logica quando logado o usuário; (iv) informações do perfil do usuário com foto; (v) agenda contendo a identificação de todos os contatos (simétricos e assimétricos) e respectivos números de telefones e imagens de perfil;

[71] Conforme: Política de Privacidade do WhatsApp. Disponível em: https://www.whatsapp.com/legal/privacy-policy/?locale=pt_BR. Acesso em 30 de dez. 2022.

[72] Nesta categoria incluem-se os dados de uso e de registro, os dados sobre conexões e dispositivos, os dados de localização e os cookies que coletam os hábitos e preferências do usuário durante a navegação na rede para personalização da experiência. Conforme a atual (última atualização em 4 de janeiro de 2021) política de privacidade do Whatsapp, os dados coletados automaticamente incluem: "Dados de uso e de registro. Coletamos dados sobre sua atividade em nossos Serviços, como dados de serviços, de diagnóstico e de desempenho. Essa coleta inclui dados sobre sua atividade (inclusive como você usa nossos Serviços, suas configurações dos Serviços, como você interage com outras pessoas usando nossos Serviços — inclusive quando você interage com uma empresa —, e o tempo, a frequência e a duração de suas atividades e interações), arquivos de registro, diagnóstico, falha, site, bem como relatórios e registros de desempenho. A coleta também inclui dados sobre quando você se cadastrou para usar nossos Serviços; os recursos que você usa, como nossos recursos de grupos, Status, ligações ou mensagens (incluindo nome do grupo, imagem do grupo e descrição do grupo), recursos comerciais e de pagamentos; foto de perfil; recado; se você está online; quando usou nossos Serviços pela última vez (seu "visto por último"); e quando você atualizou seu recado pela última vez. Dados sobre conexões e dispositivos. Coletamos dados específicos sobre conexões e dispositivos quando você instala, acessa ou usa nossos Serviços. Essa coleta inclui informações como modelo de hardware, informações do sistema operacional, nível da bateria, força do sinal, versão do aplicativo, informações do navegador, rede móvel, informações de conexão (incluindo número de telefone, operadora de celular ou provedor de serviços de internet), idioma e fuso horário, endereço IP, informações de operações do dispositivo e identificadores (inclusive identificadores exclusivos para Produtos das Empresas da Meta associados ao mesmo dispositivo ou conta). Dados de localização. Nós coletamos e utilizamos dados precisos de localização com sua permissão quando você escolhe usar recursos relacionados à localização, como quando você decide compartilhar sua localização com seus contatos ou visualizar as localizações próximas ou localizações que outras pessoas compartilharam com você. Há determinadas configurações relacionadas a dados de localização que você pode encontrar nas configurações do seu dispositivo ou do aplicativo, como o compartilhamento de localização. Mesmo se você não utiliza nossos recursos relacionados à localização, usamos endereços IP e outros dados como códigos de área de número de telefone para calcular sua localização geral (por exemplo, cidade e país). Nós também usamos seus dados de localização para fins de diagnóstico e de solução de problemas. Cookies. Usamos cookies para operar.

(vi) informações dos grupos, como descrição, nome identificação do grupo (Group-ID), data de criação e lista de membros, quem criou o grupo e seus administradores, entre outras.[73][275]

Ainda no caso do WhatsApp, uma medida particularmente interessante e que já vem sendo praticada é a possibilidade de obtenção de extratos das mensagens trocadas entre usuários do aplicativo a cada período de 24h, contatos a partir da implementação da decisão judicial (logo, é inviável a obtenção destes dados para o passado) (Wendt; Jorge, 2021, p. 141). Os extratos conterão "1. informações sobre remetente, número do telefone do destinatário, data, hora e fuso horário das mensagens; 2. registro de conexão de ambos os interlocutores, listando o endereçamento do IP de cada uma das trocas de mensagem [...] 3. tipo de mensagem trocada entre os interlocutores, a exemplo de saber se foi enviado um arquivo de imagem, áudio, vídeo" (Figueiredo Júnior; Patury, 2022, p. 286).

Em síntese, o WhatsApp coleta dos usuários informações sobre sua localização, atualizações de status, detalhes do seu provedor de serviços de Internet, endereço IP, contatos, modelo do celular, histórico de compras, dados de falhas do sistema, dados de desempenho e interação junto com sua foto de perfil e número de celular.

A situação do Telegram é distinta à do Whatsapp[74], a começar pela arquitetura do sistema,[75] no qual apenas chats secretos, chamadas de voz e videochamadas são protegidos por

[73] Figueiredo Júnior, Jorge Figueiredo; Patury, Fabrício Rabelo. Quebra telemática de whatsapp e sua utilização no combate ao crime organizado. In: Paulino, Galtiênio da Cruz, et al. Técnicas avançadas de investigação, 2º volume. Brasília: ESMPU, 2022. p. 286. No mesmo sentido: Jorge, Higor Vinicius Nogueira; Fonseca, Ricardo Magno Teixeira. Fraudes com o auxílio da tecnologia e relevância da investigação criminal tecnológica. In: vergine, Gaetano; Jorge, Higor Vinicius Nogueira. Relatos sobre a investigação de crimes cibernéticos. Salvador: Juspodivm, 2022. p. p. 151-152. Disponível em: https://www.editorajuspodivm.com.br/relatos-sobre-a-investigacao-de-crimesciberneticos-2022. Acesso em: 02 jan 2023.

[74] As diferenças são pontuadas expressamente pelo próprio Telgram: "Ao contrário do WhatsApp, o Telegram é um mensageiro baseado em nuvem com sincronização contínua. Como resultado, você pode acessar suas mensagens de vários dispositivos ao mesmo tempo, incluindo tablets e computadores, e compartilhar um número ilimitado de fotos, vídeos e arquivos (doc, zip, mp3, etc.) de até 2 GB cada. E se você não quiser armazenar todos os dados no seu dispositivo, você pode sempre mantê-los na nuvem. Graças à nossa infraestrutura de múltiplos data centers e criptografia, o Telegram é mais rápido e muito mais seguro. Além disso, conversas privadas no Telegram são gratuitas e continuarão gratuitas — sem anúncios, sem taxas de assinatura, para sempre." Disponível em < https://telegram.org/faq/br#p-qual-a-diferenca-do-telegram-para-o-whatsapp> Acesso em 30 dez. 2022.

[75] Segundo o Telegram, são oferecidas duas camadas de criptografia segura: "A criptografia clienteservidor, que é usada em chats na nuvem (chats privados e em grupo). Os chats secretos usam uma camada adicional de criptografia cliente-cliente. Todos os dados, independentemente do tipo, são criptografados da mesma maneira — seja texto, mídia ou arquivos. Nossa criptografia é baseada em criptografia AES simétrica de 256 bits, criptografia RSA de 2048 bits e troca de chaves segura DiffieHellman." Disponível em <https://telegram.org/faq/br#p-entao-como-voces-criptografam-os-dados> Acesso em 30 dez. 2022.

criptografia de ponta a ponta[76] (logo, não há criptografia de ponta a ponta por padrão). A criação de conta no aplicativo exige que usuário registre um número válido de telefone, que deverá ser acrescido do registro do e-mail em caso de habilitação da verificação em duas etapas. Ao contrário do Whatsapp, que, como regra, não armazena as mensagens em seus servidores (que ficam apenas nas pontas da comunicação), o Telegram armazena dados de conteúdo das mensagens trocadas em seus data centers, independentemente de backups, o que viabilizaria, ao menos em tese, o acesso remoto por autoridades de persecução. Segundo sua política de privacidade, Telegram coleta e armazena metadados (endereço IP, dispositivos e aplicativos que utilizam o Telegram, histórico de alterações de nomes de usuário) por até 12 meses[77]. Ocorre que o Telegram adota uma política de informação zero e chega a anunciar, sem qualquer embargo, suas estratégias para inviabilizar o acesso ao conteúdo dos chats, bem como o orgulho de não divulgar dados de usuários para terceiros ou governos[78]. Senão vejamos:

> Para proteger os dados que não são cobertos pela criptografia de ponta a ponta, o Telegram usa uma infraestrutura distribuída. Os dados dos chats em nuvem são armazenados em vários data centers em todo o mundo, controlados por diferentes entidades jurídicas espalhadas por diferentes jurisdições. As chaves de decodificação relevantes são divididas em partes e nunca são mantidas no mesmo lugar que os dados que elas protegem. Como resultado, várias ordens judiciais de diferentes jurisdições são necessárias para nos obrigar a desistir de quaisquer dados. Graças a essa estrutura, podemos garantir que nenhum governo ou bloco de países com idéias afins possa invadir a privacidade e a liberdade de expressão das pessoas. O Telegram só pode ser forçado 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, divulgamos 0 bytes de dados de usuários para terceiros, incluindo governos. (grifo nosso)[79]

Contraditoriamente, a política de privacidade do Telegram ressalta, textualmente, que se forem recebidas ordens judiciais de um país democrático, como o Brasil, em relação ao uso da plataforma do Telegram para atividades proibidas pelos termos de uso ou que se refiram à apuração de infrações graves como terrorismo e abusos contra crianças e adolescentes, os "endereços de IP e números de telefone de suspeitos podem ser disponibilizados para as autoridades competentes".[80]

---

[76] Perguntas frequentes. Disponível em https://telegram.org/faq?setln=pt-br Acesso em 30 dez. 2022
[77] Conforme https://telegram.org/privacy/br Acesso em: 08 jan. 2023
[78] Conforme Perguntas frequentes. Disponível em: https://telegram.org/faq?setln=pt-br. Acesso em 30 dez. 2022.
[79] Conforme Perguntas frequentes. Disponível em: https://telegram.org/faq?setln=pt-br. Acesso em: 30 dez. 2022
[80] Conforme Política de Privacidade do Telegram. Disponível em: https://telegram.org/privacy/br. Acesso em 30 dez. 2022.

Já se viu, contudo, que o Telegram colaborou com Supremo Tribunal Federal no caso da Petição 9.935. Recentemente, o aplicativo também cooperou com o sistema de justiça indiano ao divulgar nomes, números de telefone e endereços IP de usuários acusados de compartilhar material ilícito por violação de direitos autorais.

O Signal também se destaca em popularidade[288] entre os aplicativos de mensageria criptografadas de ponta a ponta, sobretudo após modificação da política de privacidade do Whatsapp em janeiro de 2021[81], que provocou verdadeiro êxodo de usuários mundialmente noticiado nas em mídias especializadas[290]. Trata-se de uma aplicação que utiliza código aberto[291] e que incorpora grande parte dos recursos já disponíveis no WhatsApp, com algumas funcionalidades adicionais como: (i) trocar as chaves de uma sessão, ainda que não haja resposta para a mensagem enviada; (ii) faculdade de inviabilizar a captura de tela; (iii) a faculdade de utilização senhas específicas para certos chats de conversa; (iv) e uma criptografia ponta a ponta de tal modo abrangente que tornaria praticamente impossível a sua violação se comparada a outras tipologias.[82] O aplicativo é considerado um dos mais seguros do gênero[83], se notabilizando por criptografar inclusive metadados de comunicação sobre os

[81] "De acordo com dados da empresa de análise Sensor Tower, o Signal foi baixado 246.000 vezes em todo o mundo na semana anterior ao WhatsApp anunciar a mudança em 4 de janeiro e 8,8 milhões de vezes na semana seguinte. Na Índia, os downloads passaram de 12.000 para 2,7 milhões. No Reino Unido, saltaram de 7.400 para 191.000, e nos Estados Unidos de 63.000 para 1,1 milhão.Na quartafeira, o Telegram disse que ultrapassou 500 milhões de usuários ativos em todo o mundo. Os downloads saltaram de 6,5 milhões na semana iniciada em 28 de dezembro para 11 milhões na semana seguinte.
Durante o mesmo período, os downloads globais do WhatsApp diminuíram de 11,3 milhões para 9,2 milhões." Disponível em: https://www.bbc.com/news/technology-55684595. Acesso em: 28 dez 2022. [290] Belli, Luca; Zingales, Nicolo. Novas Regras do WhatsApp: a proteção de dados se torna um luxo para 2 bilhões de pessoas? Disponível em: https://mittechreview.com.br/novas-regras-defacebook-e-whatsapp-a-protecao-de-dados-se-torna-um-luxo-para-2-bilhoes-depessoas/#TB_inline?height=300&width=400&inlineId=single-pdf-download. Acesso em: 20 dez. 2022. [291] Os softwares de código aberto se notabilizam por ter seu código disponível publicamente e apresentarem poucas falhas ou vulnerabilidades, já que admitem que auditorias (por qualquer interessado normalmente membros da academia e de comunidades que apoiam o software livre) testem a higidez dos sistemas, viabilizando a rápida identificação e correção de problemas eventualmente detectados. O código do signal encontra-se disponível em: https://github.com/signalapp. Acesso em: 20 de dez. 2022.

[82] Como funciona o app 'ultrasseguro' de mensagens usado por Snowden. 2016. Disponível em: https://www.bbc.com/portuguese/geral-37821449. Acesso em: 18 mar. 2022.

[83] 293 Signal: entenda por que o aplicativo de mensagens é considerado ultrasseguro. 2019. Disponível em: https://www.estadao.com.br/link/signal-entenda-por-que-o-aplicativo-de-mensagense-considerado-ultrasseguro/. Acesso em: 31 de dez de 2022. Ainda assim, o Signal não está imune a ataques e recentemente (15 de agosto de 2022) a equipe do Signal informou um ataque por hackers desconhecidos. A investida não teria logrado êxito em acessar o conteúdo das mensagens e os contatos dos alvos, haja vista, primeiramente, que no sistema criptográfico de ponta a ponta do signal as mensagens trocadas por usuário ficam armazenadas tão somente em seus dispositivos (e não nos data centers), razão pela qual fica impossível o acesso apenas hackeando a infraestrutura; além disso, "O que é armazenado nos servidores do Signal são os números de telefone dos usuários, bem como os números de telefone de seus contatos. Isso permite que o aplicativo notifique quando um contato seu se inscrever no Signal. No entanto, os dados são armazenados, primeiro, em armazenamentos especiais chamados enclaves seguros, que nem mesmo os desenvolvedores do Signal podem acessar. E segundo, os próprios números não são armazenados em texto simples, mas na forma de um código

interlocutores envolvidos na troca de mensagens (Lee, 2016). Os únicos metadados[84] disponíveis no Signal são a data e a hora de inscrição do usuário na aplicação e a data do último login no aplicativo (Kroll, 2021), de modo que até os dados do perfil[85][297] do usuário e seus contatos[86] ficam abarcados por criptografia de ponta a ponta.[87, 88]

Em documento obtido diretamente do FBI (Kroll, 2021) pela Property of the People[89] (e replicado em mídias especializadas em todo o mundo), associação privada, com base na Lei de Liberdade de Informação americana, consta que mediante ordem judicial a Apple pode fornecer informações (i) básicas do assinante-alvo, (ii) dados sobre consultas realizados no iMessage dos últimos 25 dias, (iii) o que um usuário visualizou no iMessage e também (iv) quais outras pessoas pesquisaram o nome do usuárioalvo no aplicativo.[90]

---

hash. Esse mecanismo permite que o aplicativo Signal em seu telefone envie informações criptografadas sobre os contatos e receba uma resposta também criptografada sobre qual de seus contatos usa o Signal. Em outras palavras, os invasores também não conseguiram acessar a lista de contatos do usuário."
(John Snow. Signal é seguro. Quem comprova são os hackers.2022. Disponível em <https://www.kaspersky.com.br/blog/signal-hacked-but-still-secure/19942/>)

[84] Para mais informações sobre a criptografia dos metadados pelo signal, vide https://signal.org/blog/sealed-sender/ Acesso em: 31 de dez de 2022

[85] Afirma o Signal que quando é criado um novo perfil, a imagem e o nome escolhidos são criptografados utilizando uma chave de perfil exclusiva. O conteúdo do perfil criptografado é carregado no servidor (que nunca tem acesso à chave do perfil). Assim, durante uma conversa normal, o usuário do Signal compartilhará com segurança sua chave de perfil personalizado com outros usuários com autorização para visualização das informações do perfil. Disponível em https://signal.org/blog/signalprofiles-beta/ Acesso em: 20 de dez. 2022.

[86] Conforme https://signal.org/blog/private-contact-discovery/ Acesso em: 20 de dez. 2022

[87] Assim consta nos na política de Privacidade do Signal: "Informação da conta. Você registra um número de telefone quando cria uma conta do Signal. Os números de telefone são usados para fornecer nossos Serviços a você e a outros usuários do Signal. Você pode, opcionalmente, adicionar outras informações à sua conta, como um nome de perfil e uma foto de perfil. Essas informações são criptografadas de ponta a ponta ." Disponível em < https://signal.org/legal/#privacy-policy>. Acesso em: 20 dez 2022.

[88] Note-se que com informações de hora de inscrição e último login (conjugada ou isoladamente) é possível inferir se o aplicativo está sendo usado. Em tese, é possível ainda que se retenha dados prospectivos de últimos acessos ao aplicativo, de modo a circunscrever padrões de acesso ao signal e a indisponibilizar o sistema para um usuário específico para forçá-lo a utilizar outro meio de comunicação menos protegidos não protegido, como ligações convencionais.

[89] Esse tipo de acesso não é raro de acontecer nos EUA em relação às práticas investigativas do FBI. Anos após os ataques de San Bernardino, descobriu-se como o FBI teve acesso aos celulares criptografados, bem como não é totalmente desconhecida a tática da agência de resguardar os segredos de suas práticas investigativas tecnológicas. Conforme: HEATH, Brad. FBI warned agents not to share tech secrets with prosecutors. 2016. Disponível em: https://www.usatoday.com/story/news/2016/04/20/fbi-memos-surveillance-secrecy/83280968/. Acesso em: 31 dez. 2022.

[90] Apesar do maior detalhamento constante no documento, nota-se que está alinhado com os termos da política de privacidade, que assim traz: "Informações básicas sobre clientes ou cadastros, inclusive nome, endereço, endereço de e-mail e número de telefone, são fornecidas à Apple quando um cliente associa um aparelho a um ID Apple. [...] As informações de registro, caso estejam disponíveis, poderão ser obtidas mediante a solicitação judicialmente válida pertinente para o país do solicitante. [...] As comunicações do iMessage são criptografadas de ponta a ponta, e a Apple não tem como decodificar os dados do iMessage quando estão em trânsito entre os aparelhos. A Apple não intercepta as comunicações do iMessage nem tem os registros das comunicações do iMessage. A Apple dispõe de registros de consultas de recursos do iMessage. Esses registros indicam que uma consulta foi iniciada por um aplicativo do aparelho (Mensagens, Contatos, Telefone, etc.) e encaminhada para os servidores da Apple em busca de um identificador de pesquisa (o qual pode ser um número de telefone,

Intitulado "acesso legal", o documento aborda a capacidade do FBI de acessar licitamente o conteúdo e alguns metadados gerados por nove aplicativos de mensageria privada (iMessage, Line, Signal, Telegram, Threema, Viber, WeChat, WhatsApp e Wickr). Em relação aos metadados, consta que "os dados fornecidos pelas empresas listadas abaixo, com exceção do WhatsApp, são na verdade logs de acesso que são fornecidos às autoridades, não em tempo real, e podem afetar as WhatsApp, o documento traz uma informação que contrasta fortemente com a realidade brasileira em relação ao tempo de resposta (24h, como regra) do provedor para envio da massa de metadados às autoridades de persecução. Segundo consta, com um "pen register"[91] o tempo de envio dos dados pelo Whatsapp ocorre com atualizações periódicas dos dados de origem e destino das mensagens a cada 15 minutos (praticamente em tempo real), o que foi conformado por porta voz do WhatsApp após a repercussão da mídia internacional.

Por tudo que se viu até aqui, nota-se que as principais vantagens da análise de metadados gerados nas comunicações por aplicações de mensageria como alternativa à falta de acesso ao conteúdo das comunicações digitais são a sua: (i) disponibilidade, porquanto apresentam-se normalmente em formato legível; (ii) estruturação[92], já que os metadados normalmente são arquivos mais leves que o conteúdo das mensagens (que podem incluir mídia ou caracteres especiais) e que deixam pouca margem de interpretação (por versarem, como visto, sobre data, hora, localização e quantidade de mensagens trocadas), o que facilita o processamento e cruzamento de informações para produção do conhecimento forense; [93] (iii) guarda obrigatória.

---

endereço de e-mail ou ID Apple) para determinar se esse identificador de pesquisa é "compatível com o iMessage". [...] Os registros de consultas de recursos do iMessage são retidos por até 25 dias. Esses registros, caso estejam disponíveis, poderão ser obtidos mediante a solicitação judicialmente válida pertinente para o país do solicitante." Embora o conste que a Apple não retenha registros das comunicações travadas no iMessage, o seu guia para autoridades de persecução indica que poderão ser obtidos os registros da "atividade de conexão de um cliente ou aparelho com os serviços da Apple, como Apple Music, app Apple TV, Apple Podcasts, Apple Books, iCloud, Meu ID Apple e Fóruns da Apple", mediante a solicitação judicialmente válida pertinente para o país do solicitante. Disponível em <https://www.apple.com/legal/privacy/law-enforcement-guidelines-outside-us-br.pdf> Acesso em: 21 de dez. 2022

[91] Dispositivo ou ferramenta eletrônica usada para capturar dados sobre comunicações eletrônicas ou digitais. (Tatum, Malcolm. What is a Pen Register? dezembro de 2022. Disponível em < https://www.easytechjunkie.com/what-is-a-pen-register.htm> Acesso em: 21 de dez. 2022

[92] Campos, Luiz Fernando de Barros. Metadados digitais: revisão bibliográfica da evolução e tendências por meio de categorias funcionais. Encontros Bibli: revista eletrônica de biblioteconomia e ciência da informação, [S. l.], v. 12, n. 23, p. 17, 2007. DOI: 10.5007/15182924.2007v12n23p16. Disponível em: https://periodicos.ufsc.br/index.php/eb/article/view/15182924.2007v12n23p16. Acesso em: 11 jan. 2023.

[93] Assembleia Geral da Onu. 2014. Nova York. O direito à privacidade na era digital: Relatório do Gabinete do Alto Comissariado das Nações Unidas para os Direitos Humanos. 27ª sessão do

No Brasil, a obrigação de guarda e entrega de metadados está espalhada por distintas leis[94308]. Dentro do recorte dos aplicativos de mensageria, particularmente relevante é o dever de guarda dos registros de acesso à aplicação pelos provedores de aplicações de internet constituídos como pessoa jurídicas que exerçam atividade organizada, profissional e com fins econômicos, sendo que os registros deverão ser mantidos sob sigilo, em ambiente controlado e seguro pelo prazo de seis meses. Note-se que o alvo do dever de guarda não qualquer provedor de aplicação, mas tão somente os que desempenhem suas atividades empresarialmente. Já os provedores de aplicação não empresariais poderão ser compelidos judicialmente a guardar, os registros de acesso a aplicações, desde que se trate de registros relativos a fatos específicos em período determinado (§ 1º do art. 15). O Marco Civil possibilita também que autoridades policiais ou administrativa ou os membros do Ministério Público requeiram "cautelarmente" a guarda dos registros de acesso a aplicações, inclusive por prazo superior a seis meses. Em qualquer hipótese, a disponibilização dos registros de acesso deverá ser precedida de autorização judicial. No caso da guarda cautelar requerida pelas autoridades de persecução, o acesso ao conteúdo guardado pelo provedor fica condicionado ao prazo peremptório de sessenta dias para ingresso da respectiva medida judicial (quebra do sigilo de metadados).

---

Conselho de Direitos. Nova York. 2017. p. 198-199. Disponível em <https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F27%2F37&Language=E&DeviceType=Desktop&LangRequested=False>. Acesso em: 20 dez. 2022

[94] 308 Os provedores de telefonia fixa e móvel são obrigados a manter à disposição do Ministério Público e dos delegados de polícia, por 5 anos, os "registros de identificação dos números dos terminais de origem e de destino das ligações telefônicas internacionais, interurbanas e locais" (art. 17 da Lei 12.850/13); os provedores de conexão à Internet devem armazenar por um ano os registros de conexão, isto é o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados" (art. 5º, VI, e 13 do MCI); a Lei de Lavagem de Dinheiro determina que os dados e informações cadastrais de investigados (qualificação pessoal, filiação e endereço) devem ser mantidos pela Justiça Eleitoral, pelas empresas telefônicas, pelas instituições financeiras, pelos provedores de internet e pelas administradoras de cartão de crédito, para acesso da autoridade policial e o Ministério Público, independentemente de autorização judicial (art. 17-B da lei 9616/98); O Código de Processo Penal (art. 13-A e 13-B) possibilita o acesso a dados cadastrais sem ordem judicial, bem como a "sinais" de localização, com autorização judicial, no caso de crimes de maior gravidade. Saliente-se que a obtenção de registros telefônicos e outros metadados produzidos por meio das comunicações telefônica (localização) não dispõe de regulamentação por meio de lei específica, razão pela qual o acesso a tais dados se dá por meio de autorização judicial para a produção probatória. Registre-se, por fim que o Supremo Tribunal Federal já decidiu ser possível a obtenção de registros telefônicos também por Comissões Parlamentares de Inquérito (BRASIL. Supremo Tribunal Federal. Tribunal Pleno. Mandado de Segurança nº 23452/RJ. Comissão Parlamentar de Inquérito. Poderes de investigação. limitações constitucionais. legitimidade do controle jurisdicional. Possibilidade de a CPI ordenar, por autoridade própria, a quebra dos sigilos bancário, fiscal e telefônico. Necessidade de fundamentação do ato deliberativo. Deliberação da CPI quem sem fundamentação, ordenou medidas de restrição a direitos. Mandado de Segurança deferido. Impetrante: Luiz Carlos Barretti Júnior. Impetrado: Presidente da Comissão Parlamentar de Inquérito. Relator:.Ministrp Celso de Mello. Data da Decisão: 16 de set. 1999).

Na própria dicção literal do Marco Civil, considera-se aplicações de internet "o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet" (Brasil, 2014)[95], sendo que os registros de acesso a aplicações de internet são "o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP."[310] (artigo 5º, VII e VIII, do MCI)

Por ocasião da audiência pública realizada no âmbito da ADPF 403 e da ADI 5527, o acesso à metadados foi apontado em diversas oportunidades como alternativa investigativa em substituição ao acesso ao conteúdo da comunicação[96311], fazendo coro ao discurso contra a fragilização da criptografia por meio da criação de mecanismos de acesso excepcional.[97] Acerca da importância dos metadados para investigações, veja-se como se manifestou Fernanda Domingos, Procuradora da República, na audiência pública (Brasil, 2014):

> [...] embora o objeto das ações não discuta diretamente criptografia e fornecimento de conteúdo de metadados, são questões subjacentes ao descumprimento das ordens judiciais que ensejaram os bloqueios do aplicativo WhatsApp, pois são relevantes para as investigações de crimes seríssimos, é preciso lembrar, como tráfico de drogas, de armas e de pessoas, troca de pornografia infantil, preparação de sequestro, de homicídios e de atentados terroristas, dentre outros. [...] Com relação aos metadados, o WhatsApp nos informou, em janeiro, que passou a reter os metadados - que são as informações criadas em cada transmissão de mensagens. [...]Nós não conseguimos comprovar ainda se, de fato, isso está sendo cumprido, como eles disseram, mas é importante demonstrar como é necessário haver uma sanção prevista em lei, como está no Marco Civil, para que os direitos ali assegurados sejam garantidos." (grifo nosso)

Saliente-se que a utilização de metadados já contribuiu para o êxito em investigações de grande repercussão nacional, a exemplo dos casos dos assassinatos da Magistrada Patrícia Acioli (em 2011) e da vereadora Marielle Franco e do motorista Anderson Gomes (em 2018). No caso do assassinato da Juíza Patrícia Acioli, os investigadores recuperaram e analisaram uma grande quantidade de metadados telefônicos que conduziram à identificação dos Policiais

---

[95] Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 01 jan. 2023.

[96] O perito da Polícia Federal, Ivo Peixinho, asseverou: "Propõe-se que a empresa forneça metadados, que acreditamos que ela disponha, mediante ordem judicial referente a um caso em investigação [...], com a possibilidade talvez de notificar conteúdo relacionado a pornografia infantil, quando forem compartilhados elementos de mídia, como imagens e vídeos" (p. 21-22); Transcrição disponível em: <http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADI5527ADPF403AudinciaPblicaMarco CivildaInterneteBloqueioJudicialdoWhatsApp.pdf>. Acesso em: 31 de março de 2021.

[97] Defendem os metadados como alternativa ao enfraquecimento à criptografia: Abelson et al., 105, p. 3; Carnegie, 2019, p. 5; Gill et al., 2018, p. 22; Lewis et al., 2017, p. 35; Kuehn, Mcconnell, 2018, p. 24; Castro, Mcquinn, 2016, p. 25; Nasem, 2018, p. 45, 71; Swire, Ahmad, 2012, p. 467.

Militares responsáveis pelo crime[98]. No homicídio da vereadora Marielle Franco e do motorista Anderson, para se chegar aos executores do crime foram analisados conjugadamente uma enormidade de dados de localização de aparelhos celulares, históricos de navegação e centenas de gigabytes de metadados (Padrão, 2019).

Importa registrar, contudo, que a criptografia não é a única barreira técnica que autoridades de persecução enfrentam para alcançar o conteúdo de mensagens trocadas em aplicativos de mensageria e os metadados gerados nessas comunicações. Ainda quando a criptografia não esteja presente, o acesso ao texto sem formatação pode ser precedido de outros obstáculos técnicos. Isso se dá em função de o texto simples e os metadados não poderem ser acessados sem a compreensão dos múltiplos protocolos, algoritmos e formatos utilizados pelos aplicativos, haja vista que tais elementos nem sempre se encontram bem documentados e estão sujeitos a frequentes alterações. Acaso a agência de investigação não disponha de recursos técnicos robustos ou da cooperação provedor de aplicação, certamente as investigações ficarão comprometidas (National Acedemies of Sciences, 2018. p. 6). A dificuldade prática está presente na realidade brasileira, como bem retratam Wendt e Jorge (2021, p. 146):

> Importante considerar que as informações são apresentadas em um formato que dificulta a sua compreensão, sendo importante utilizar ferramentas analíticas que tornem mais acessíveis as informações, como, por exemplo, a consulta bilhetagem oferecida no Portal Inteligência Info, da Polícia Civil do Ceará que apresenta as informações em um layout mais compreensível para aquele que recebe as informações oriundas do WhatsApp. Importante ressaltar que atualmente basta cadastrar o e-mail do policial civil no Portal Inteligência da Polícia Civil do Ceará, independente do estado da federação do policial, de modo que ele terá acesso a referida funcionalidade, além de outras ferramentas e orientações.

[98] Investigação de morte de juíza fecha o cerco sobre policiais acusados de crimes. Veja. 2011. Disponível em: https://veja.abril.com.br/brasil/investigacao-de-morte-de-juiza-fecha-o-cerco-sobrepoliciais-acusados-de-crimes/; e Justiça mantém penas de seis PMs envolvidos na morte de juíza no Rio. Folha de S. Paulo. 2016. Disponível em: https://www1.folha.uol.com.br/cotidiano/2016/10/1820061-justica-mantem-penas-de-seis-pmsenvolvidos-na-morte-de-juiza-no-rio.shtml. Acesso em: 31 de dez de 2022.

## 3.4 MEDIDAS DE PERSECUÇÃO PENAL PARA ACESSO ÀS COMUNICAÇÕES DIGITAIS - INTERCEPTAÇÃO TELEMÁTICA E QUEBRA DE SIGILO DE DADOS: BREVES COMENTÁRIOS.

Dentre as técnicas à disposição dos órgãos de persecução penal para acesso[99] e registro de dados/evidências digitais, destacam-se duas medidas, especialmente relevantes e igualmente distintas, que foram o cerne das ordens de bloqueios do aplicativo WhatsApp: a interceptação do fluxo das comunicações (telefônicas ou telemáticas) e a quebra de sigilo de dados estáticos. A normativa de regência varia para cada uma das medidas, segundo a sua natureza específica.

As medidas de interceptação das comunicações são caracterizadas pela "intervenção de um terceiro, que desvia, em tempo real e sem o conhecimento dos interlocutores, o conteúdo de mensagens representadas por sons ou símbolos, registrando-os para fins de prova" (Pezzotti, 2022. p. 242). O dispositivo constitucional de regência da medida é o art. 5º, XII, da CF, que textualiza o direito fundamental à inviolabilidade do sigilo das comunicações: "é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados [100][320] e das comunicações telefônicas, salvo, no último caso[101], por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal" (Brasil, 1988).

---

[99] Em razão do recorte do presente trabalho, exclui-se deste tópico o acesso a comunicações armazenadas em dispositivos físicos pessoais que possam ser facilmente apreendidos, como smartphones, tablets, computadores, entre outros, os quais recebem tratamento jurídico diverso (que varia a depender se a apreensão do dispositivo deriva de prisão
em flagrante ou de medida cautelar probatória de busca e apreensão).

[100] Há divergências interpretativas sobre o espectro alcance do dispositivo em relação ao termo "dados". Para alguns o termo designaria tão somente a comunicação de dados, para outra parcela da doutrina, o inciso tutelaria além da comunicação de dados, também os dados em si (ou seja, os dados estáticos, em repouso). Antonio Scarance Fernandes divisa do último entendimento e ensina que âmbito de tutela do inciso deveria resguardar também os dados estáticos, mas anota uma análise sistemática do teor do dispositivo que conduz inevitavelmente à conclusão de que "todo o inciso protege inviolabilidades de comunicações – por correspondência, por telégrafo e por telefone – e, assim, a intenção do legislador seria também a de proteger a comunicação dos dados e não a estes em si mesmos" (Fernandes, 2007, p. 17 e 21). Na jurisprudência do Supremo Tribunal Federal, há muito é assente o entendimento de que o inciso resguarda apenas as comunicações de dados, os dados em fluxo, e não dados em repouso. Nesse sentido: Brasil. STF. Tribunal Pleno. RE 418.416. Relator: Min. Sepúlveda Pertence, julg.10.5.2006. DJ 19 dez. 2006 e Brasil. STF. Tribunal Pleno. RE 418.416. Relator: Min. Sepúlveda Pertence, DJ 19 dez. 2006; BRASIL. STF. Primeira Turma. HC 124.322-AgR. Relator: Min. Roberto Barroso, DJe de 19 dez. 2016; BRASIL. STF. Primeira Turma. AgR RHC 169.682. Relator: Min. Luiz Fux, julg. 3.4.2020, processo eletrônico, DJe 117, divulg. 11.5.2020, public. 12 maio 2020).

[101] A interpretação de "no último caso" também rendeu ensejo às divergências doutrinárias acerca de quais tipologias de comunicação elencadas no inciso estariam abrangidas pela possibilidade de interceptação. Pacificou-se na jurisprudência, contudo, que a exceção ao sigilo das comunicações contemplaria não só as comunicações telefônicas, mas também as comunicações de dados telemáticos (por todos, veja-se: BRASIL. Supremo Tribunal Federal. Segunda Turma. RHC 132.115. Relator: Min. Dias Toffoli, julg. 6.2.2018, processo

A regulamentação infraconstitucional das hipóteses e formas de intervenção nas comunicações ficou a cargo da Lei n. 9.296/1996. O próprio texto constitucional traz a limitação material do instrumento, que se destina à investigação criminal ou instrução processual penal. O objeto da medida interceptação é captação das comunicações telefônicas e telemáticas, presente e futura, em outras palavras: o fluxo das comunicações.

Segundo Ada Pelegrini Grinover, o termo "telemática", empregado pelo parágrafo único do art. 1º da Lei n. 9.296/1996, consiste na "[...]manipulação e utilização da informação através do uso combinado do computador e meios de telecomunicação" (Grinover, 1997, p. 115). Trata-se, em suma, da "[...]fusão das técnicas de telefonia – aparelhos telefônicos, cabos de telecomunicação, satélites e cabos de fibra ótica, por exemplo – com o tratamento informatizado de dados pelo emprego de dispositivos informáticos, softwares e sistemas de redes" (Pezzotti, 2022, p. 244). O termo "dados" mencionado no dispositivo refere-se exclusivamente a "dados digitais", que pode ser definido como "conjunto de signos de estrutura numérica e imaterial, processado por sistemas computacionais, voltado a desempenhar uma função e representado em diversos modelos informativos (textos, imagens, áudio e vídeo)". Simplificadamente, dados digitais são dados passíveis de processamento eletrônico.

O fato de apenas as comunicações em fluxo receberem a proteção constitucional contra a violação do sigilo (artigo 5º, XII, CF) não significa que as comunicações passadas não estejam constitucionalmente tuteladas. Digitais ou não, as comunicações passadas guardadas por uma pessoa encontrarão proteção no inciso X do artigo 5º, norma central de proteção da privacidade[102] na Constituição Cidadã de 1988 por estatuir a inviolabilidade da intimidade, vida privada, honra e imagem (Brasil, 1988).

---

eletrônico, DJe 223, divulg. 18.10.2018, public. 19 out. 2018). Saliente-se que no mesmo ano em que a Lei n. 9.296/1996 entrou em vigor, foi ajuizada a Ação Direta de Inconstitucionalidade 1.488-9/DF impugnando a extensão da possibilidade de interceptações para as comunicações telemáticas, todavia a ADI foi extinta sem julgamento do mérito por falta de legitimidade ativa ad causam. Em 2008 foi ajuizada a Ação Direta de Inconstitucionalidade 4.112/DF questionando, dentre outros, o mesmo ponto guerreado, a qual ainda está pendente de julgamento.

[102] Diante do fenômeno da digitalização, é cediço que a revelação não autorizada de dados armazenados de uma pessoa pode resultar em grave violação da privacidade, porquanto podem abranger informações sensíveis como documentos médicos, dados bancários e fiscais, imagens da vida privadas, dados sobre a localização, e-mails, backups de diálogos, dentre outros. Logo, nada mais natural que a tutela da privacidade alcance os backups de diálogos travados em aplicativos de mensageria privada.

Como consequência prática dos distintos paradigmas da tutela constitucional de dados digitais em fluxo e armazenados, tem-se que a disciplina da Lei n. 9.296/1996 não alcança os últimos, ainda que se trate de dados comunicacionais, a exemplo das conversas por aplicativos.

No plano infraconstitucional, a LGPD consignou expressamente a inaplicabilidade do seu regime jurídico ao tratamento de dados pessoais para fins de atividades de segurança pública, investigação criminal e repressão a infrações penais.

A disciplina legal do acesso a dados estáticos para fins penais coube ao Marco Civil da Internet, que preconiza serem invioláveis e sigilosas as comunicações privadas armazenadas, ressalvada a hipótese de ordem judicial (artigo art. 7º, III).

A seção III, do terceiro capítulo do Marco Civil da Internet, traz as normas de proteção aos registros, dados pessoais e às comunicações privadas, constando do artigo 10[103] os diversos tipos de dados digitais armazenados[104] que são protegidos, a saber: (i) registros de conexão "[...] o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados" - art. 5º, VI, Lei n. 12.965/2014); (ii) registros de acesso a aplicações da internet ("[...] conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP" - art. 5º, VIII, Lei n. 12.965/2014); (iii) conteúdo de comunicações privadas; e (iv) dados pessoais (o legislador optou, acertadamente, por uma adotar uma cláusula aberta para garantir proteção ampla aos dados digitais quando estiverem vinculados a determinado usuário).

De acordo com § 1º do artigo 10 do MCI[105], os provedores responsáveis por guardar dados digitais somente serão obrigados "a disponibilizar os registros mencionados no caput",

[103] "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" (grifos nossos).

[104] Também denominados "dados estáticos", são dados em repouso, em estado inerte em meio eletrônico (servidores ou dispositivos).

[105] "§ 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".

associados ou não a dados pessoais (ou outras informações) por força de ordem judicial que observe os termos dos seus artigos 22 e 23 (Brasil, 2014), que assim preveem:

> Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.
> Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:
> I - fundados indícios da ocorrência do ilícito;
> II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e III - período ao qual se referem os registros.
> Art. 23. Cabe ao juiz tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário, podendo determinar segredo de justiça, inclusive quanto aos pedidos de guarda de registro.

Com Pezzotti (2022, p. 249), conclui-se que dos quatro tipos de dados digitais previstos no caput do art. 10, apenas três deles se encontram submetidos aos requisitos prescritos pelo artigo 22: os registros de conexão, os registros de acesso a aplicações e os dados pessoais, quando associados aos registros citados. As comunicações privadas ficaram excluídas da incidência da norma, o que tanto fica mais evidente quando se verifica previsão específica para esta modalidade de dado no mesmo artigo 10, que traz em seu § 2º, que: "[...] 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.

Vale também a transcrição do artigo 7º do MCI:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> […]
> 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; [...]

Ao remeter ao artigo 7º, incisos II e III, do MCI, a parte final do § 2º deixa claro que o acesso a dados digitais armazenados e em fluxo se submetem a distintas matizes jurídicas. É induvidoso que a lei citada no inciso II é, atualmente, a Lei 9.296/1996. Entretanto, não consta semelhante referência em relação às comunicações armazenadas, para as quais, segundo a literalidade do texto do Marco Civil, bastaria autorização judicial para acesso sem requisitos adicionais para a concessão da medida de quebra de sigilo.

Atento às distinções constitucionais e técnicas entre interceptação telemática e quebra de sigilo de dados estáticos comunicacionais, o Superior Tribunal de Justiça vem entendendo que a ausência de outros requisitos para acesso às comunicações digitais trata-se de legítima opção legislativa que "justamente no intuito de facilitar a quebra do seu sigilo" visou "ampliar a margem de discricionariedade judicial" atribuindo ao magistrado o juízo de proporcionalidade incidente que deve subsidiar a concessão da cautelar probatória, tudo em consonância com o artigo 5º, X, da CF.[106]

Mesmo muito antes da publicação do Marco Civil da internet Scarance já entendia que: "Se não estiverem os dados protegidos pelo inciso XII, estarão acobertados pelo inciso X, e, assim, poderiam ser usados quando houvesse autorização judicial com invocação do princípio da proporcionalidade ou com afirmação de justa causa" (Fernandes, 2007, p. 20). Nota-se, portanto, que a adoção de critérios de proporcionalidade (necessidade e adequação da medida) para a avaliação das hipóteses de cabimento, acrescidos dos requisitos próprios da cautelaridade (fumus comissi delicti e periculum in mora) para a concessão da medida possui boa acolhida doutrinária[107] e jurisprudencial e está alinhada com o grande potencial invasivo do acesso às comunicações digitais armazenadas em dispositivos eletrônicos.

Sempre que as técnicas de persecução penal previstas no direito pátrio possibilitarem o acesso a comunicações digitais armazenadas ou a metadados gerados pelo uso de aplicações de mensageria, sem que a implementação destas medida impliquem em írrito rebaixamento dos

---

[106] "[...]COMUNICAÇÃO PRIVADA. ARMAZENAMENTO EM CONTA DE E-MAIL. QUEBRA DO SIGILO. POSSIBILIDADE. CRIMES PUNIDOS COM DETENÇÃO. IRRELEVÂNCIA. DECISÃO JUDICIAL. PODER GERAL DE CAUTELA. TEORIA DOS PODERES IMPLÍCITOS. OMISSÃO. INEXISTÊNCIA. ART. 2º, DA LEI N. 9.296/1996. NÃO INCIDÊNCIA. ART. 7º, III, DA LEI N. 12.965/2014. APLICAÇÃO. ART. 5º, X e XII, DA CF. HARMONIA. EMBARGOS REJEITADOS [...] 2. A quebra de sigilo de conteúdo de comunicação privada armazenada em conta de e-mail depende de prévia autorização judicial, mediante decisão devidamente fundamentada, a qual, porém, diferentemente do que acontece com as interceptações telefônicas e com o fluxo de comunicações pela internet, independe dos requisitos estabelecidos no art. 2º, da Lei n. 9.296/1996, em face da incidência, específica e posterior, do previsto no art. 7º, III, da Lei n. 12.965/2014 - Marco Civil da Internet, do poder geral de cautela e da teoria dos poderes implícitos. 3. O art. 7º, III, da Lei 12.965/2014, se encontra em completa harmonia com os incisos X e XII do art. 5º da Constituição Federal, sendo legítima a sua opção de prever requisitos diferentes e mais flexíveis para a quebra do sigilo de dados privados já armazenados quando comparados com as exigências para a interceptação telefônica e de fluxo das comunicações pela internet. [...] (BRASIL, 2020) de mensageria privada criptografada deverão, justamente por força dos deveres fundamentais para com a segurança pública e administração da justiça, viabilizar o acesso às autoridades de persecução penal aos respectivos dados digitais de que disponham, respeitadas as peculiaridades da arquitetura de cada sistema criptográfico.

[107] No mesmo sentido Pezzotti defende que: "Para a decretação da medida, aplicam-se os requisitos típicos do regime de cautelaridade – fumus comissi delicti e periculum in mora. Necessita-se, portanto, de elementos que evidenciem a existência de crime e que indiquem a possibilidade de o dispositivo, conta ou servidor de armazenamento visado deterem elementos que interessem à investigação criminal, o que também demonstrará a pertinência da prova." (destaques no original) (PEZZOTTI, 2022, p. 275).

níveis de segurança (especialmente pelo enfraquecimento da criptografia) dos usuários desses sistemas informáticos, os provedores de aplicações

## 3.5 MEIOS COERCITIVOS INDIRETOS PARA COMPELIR O CUMPRIMENTO DO DEVER FUNDAMENTAL DE ENTREGA DE DADOS

Como visto, é impensável um Estado Democrático de Direito sem a presença de deveres fundamentais. Pautados na solidariedade, os deveres fundamentais integram a noção mesma de ordem democrática, a qual, ao tempo em que protege e legitima o direito, também é por ele protegida e legitimada. É por meio dos deveres fundamentais que constituições democráticas impõem condutas proporcionais a particulares, sempre com vistas à promoção de direitos fundamentais. Naturalmente, se aqueles que se encontrarem submetidos a uma determinada ordem jurídica descumprirem seus deveres fundamentais, estarão sujeitos aos respectivos sancionamentos, cuja incidência dependerá, todavia, de intermediação legislativa, porquanto tais sanções não costumam estar contempladas no texto constitucional. Embora não seja um elemento imprescindível à caracterização dos deveres fundamentais, vale destacar que a sanção é um importante instrumento coercitivo que pode estimular a eficácia social dos deveres fundamentais.

No Brasil, o texto constitucional não prevê sanções para o descumprimento dos deveres fundamentais de cooperar com a segurança pública e administração da justiça, razão pela qual deve-se recorrer às normas infraconstitucionais para investigar a existência ou não de sanções.

Em se tratando do descumprimento de decisões judiciais que determinem o acesso a dados e comunicações digitais, verifica-se que o artigo 12 do Marco Civil da Internet prevê a possibilidade de incidência das sanções de advertência, multa, suspensão temporária e proibição do exercício de atividades:

> Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;

> III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou
> IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.
> Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o caput sua filial, sucursal, escritório ou estabelecimento situado no País.

Considerado que o artigo 12 do MCI se refere a infrações do art. 10 do mesmo diploma que, de seu turno, se reporta (§ 2º) ao teor dos incisos II e III do art. 7º, tem-se por cabíveis as sansões listadas tanto nos casos de desobediência às determinações de interceptação dos fluxos das comunicações telemáticas, como nas hipóteses de resistência à entrega de dados estáticos, o que inclui comunicações eletrônicas passadas armazenadas em nuvens.

Já se viu (item 1.6) que em novembro de 2022 o STJ decidiu que empresas de internet que prestam serviços em território nacional devem se submeter à lei brasileira e manteve multa imposta por demora injustificada (considerada ato atentatório à dignidade da Justiça) ao cumprimento de decisão judicial de entrega de dados armazenados fora do território nacional, embora não por razões relacionadas à criptografia:

> [...]1. Empresas que prestam serviços de aplicação na internet em território brasileiro devem necessariamente se submeter ao ordenamento jurídico pátrio, independentemente da circunstância de possuírem filiais no Brasil. 2. O armazenamento em nuvem é estratégia empresarial que não interfere na obrigação de observância da legislação brasileira quando o serviço é prestado em território nacional. 3. A recalcitância injustificada no cumprimento de decisão judicial atrai a imposição de multa como penalização da prática de ato atentatório à dignidade da Justiça. [...]

Já se noticiou linhas acima também que o STJ possui entendimento que, além da multa, as empresas de tecnologia que desobedeçam ou retardem o cumprimento de ordens de entrega de dados à Justiça podem ser sancionadas com o bloqueio de valores pelo sistema BacenJud e inscrição em dívida ativa, mesmo na qualidade de terceiros na relação jurídica processual.[108]

[108] Não foi divulgado o número do processo em que adotado o entendimento em razão virtude da decretação de segredo judicial nos autos. A notícia extraída do sítio eletrônico do Superior Tribunal de Justiça está disponível em <https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/Alemde-multa--empresas-de-tecnologia-que-nao-fornecem-dados-a-Justica-podem-ter-valoresbloqueados-e-nome-inscrito-em-divi.aspx>. Acesso em: 2 jan. 2022.

## 4 CONSIDERAÇÕES FINAIS

De modo geral, desde a antiguidade a noção do que é público e privado é orientada segundo o contexto cultural, social, político e econômicos de cada tempo. Não por outro motivo é que o advento de novas tecnologias acaba por impactar a vida em sociedade e a própria ideia privacidade ao longo da história.

Com forte viés individualista e exclusivista até as décadas iniciais do século XX, o direito à privacidade diluiu essas características atualmente, pois assimilou valores como liberdade e livre desenvolvimento da personalidade para se adaptar às contingências decorrentes dos avanços das tecnologias de processamento eletrônico de dados.

O direito fundamental à autodeterminação informativa, que pode ser entendido como uma especificação/ampliação do núcleo do direito à privacidade, consiste em atribuir à pessoa o direito de controlar em princípio ela mesma suas informações e dados e determinar a maneira de construir a sua própria esfera privada. Controlar significa conhecer, endereçar, interromper o fluxo, controlar as formas de circulação das próprias informações.

No ordenamento jurídico pátrio, mesmo antes da Emenda Constitucional nº 115, já se entendia como implicitamente constitucionalizado o direito fundamental à autodeterminação informativa a partir de uma análise integrada de outros direitos fundamentais (especialmente privacidade e inviolabilidade de dados) e da cláusula geral de tutela da personalidade e da promoção humana.

Com a revolução digital, a necessidade de proteção de dados se intensificou. Com infinitos usos, os dados tornaram-se um valioso ativo, realidade que operou profundas transformações na própria vida em sociedade. Reflexos distintos foram, são e continuarão sendo percebidos em todos os segmentos da sociedade, e a atividade persecutória do Estado e o próprio direito não são exceções.

A massificação das formas digitais de comunicação fez da segurança on-line (proteção de dados digitais) exigência de primeira ordem para usuários. Para a garantia da segurança dos sistemas de comunicação digital, a criptografia é particularmente importante para a delimitar espaços de privacidade, de liberdade de opiniões e de expressão online, livres de ingerências

ilegais ou arbitrárias, por Estados ou outros indivíduos. Ante suas características técnicas, nota-se que a criptografia usada em aplicações de mensageria permite que os usuários possam verificar se suas comunicações estão chegando aos destinatários corretos, longe de qualquer interferência no processo, acesso não autorizado ou alteração de conteúdo.

Sob outra ótica, esta mesma criptografia forte de dados em trânsito (comunicações em fluxo) inviabiliza a condução das atividades de interceptação telemática por impedir que as autoridades de persecução consigam acessar os conteúdos de determinada comunicação em formato legível, mesmo na hipótese de os dados comunicacionais terem sido exitosamente interceptados.

A substituição das comunicações telefônicas pelas comunicações on-line via aplicações internet, aliada à assimilação da criptografia de ponta a ponta resultaram, de fato, na exclusão dos órgãos envolvidos na persecução penal do acesso ao fluxo das comunicações interpessoais.

Depois de 30 anos do início das cryptowars, de rigor reconhecer que o quadro atual do debate sobre a criptografia nas nações ocidentais de tradição democrática indica a formação de relativo consenso no sentido da sua essencialidade como instrumento de garantia de ampla gama de direitos fundamentais conectados com o sigilo de comunicações on-line.

Diante dos múltiplos usos proporcionados por aplicações de mensageria, verifica-se que medidas institucionais que de qualquer modo impliquem em rebaixamento dos níveis de segurança e/ou enfraquecimento das proteções criptográficas, devem levar em consideração o potencial exposição dos usuários e as possíveis/prováveis consequências do acesso e uso não autorizado de dados e comunicações por agentes maliciosos privados ou públicos.

Demais disso e sob o paradigma constitucional da legalidade civil, é imperioso observar que o ordenamento jurídico brasileiro não contempla regulação específica da criptografia em geral. Lado outro, alguns marcos normativos setoriais vêm reconhecendo e incentivando o uso da criptografia para proteção de dados e informações sigilosas em geral, inexistindo, até aqui, previsões normativas expressas no sentido de restringir o uso de criptografia por provedores de aplicações de internet de qualquer tipo, ou impor-lhes obrigações de entrega de chaves

criptográficas ou criação de mecanismos tecnológicos de acesso excepcional ao conteúdo de comunicações criptografadas.

Posto esse quadro, para romper qualquer estagnação do debate sobre a criptografia e viabilizar discussões mais prescritivas para problemas concretos gerados pela criptografia de ponta a ponta nas aplicações de mensageria é imprescindível, dentre outras medidas, que haja uma ampliação do foco do debate.

Nesse sentido, é salutar que as atenções se voltem ao exame de questões amplas como atualização do direito processual penal positivo e o papel do direito frente às inovações tecnológicas. Contudo, é importante que o curto prazo também faça da equação e, nessa vertente, duas questões fizeram parte de nossa investigação: (i) quais as formas/meios de adaptação das autoridades de persecução aos problemas e virtudes da mensageria criptografada, e; (ii) se/como os provedores podem/devem contribuir com a mitigação dos riscos associados (prática de crimes e encobrimento de rastros, por exemplo) à incorporação da mesma criptografia.

Para o exame das responsabilidades dos provedores de aplicação de mensageria, a teoria dos deveres forneceu importante substrato para alguns entendimentos.

Embora pouco conhecidos e estudados pela doutrina constitucional contemporânea, é impensável a construção de um verdadeiro Estado Direito sem a correlata presença de deveres que, quando extraídos diretamente da Constituição, são qualificados como fundamentais.

Com a finalidade de promover direitos fundamentais e condições dignas de vida em sociedade, os deveres fundamentais impõem condutas proporcionais a particulares (pessoas físicas e jurídicas, nacionais ou estrangeiras) que estejam submetidos a uma determinada ordem jurídica.

O dever fundamental de cooperação com a administração da justiça é um dever implícito na Constituição, extraível da análise integrada (artigo 5º, §2º, CF), dentre outros, (ii.i) da cláusula geral do devido processo legal, (ii.ii) do contraditório e ampla defesa, (ii.iii) da razoável duração do processo, (ii.iv) das características imanentes do sistema de justiça penal que, por meio do processo penal, tutela os bens jurídicos mais caros à sociedade dos ataques

intoleráveis quando a atuação dos demais ramos do direito não é suficientemente. Pode ser concretizado como necessidade da colaborar com o Poder Judiciário, cumprindo suas determinações e atendendo aos seu chamados, sem retardos injustificados e dentro das possibilidades materiais de cada pessoa.

Ao apregoar que a segurança pública é, indistintamente, responsabilidade de todos, o artigo 144 da Constituição de 1988 corporifica o dever fundamental de cooperação com a segurança pública, que também pode ser traduzido no dever de colaborar com os órgãos constitucionalmente legitimados à preservação da ordem pública e da incolumidade das pessoas e do patrimônio.

Se é certo que órgãos de persecução precisarão adaptar táticas e técnicas investigativas contínua e paralelamente ao desenvolvimento de novas tecnologias, também é inequívoco que participação dos provedores de aplicação de mensageria criptografada são essenciais para que o processo de adaptação se perfectibilize, os quais devem se desincumbir dos seus deveres fundamentais de cooperar com a segurança pública e com a administração da justiça, sempre na exata medida do que lhes for técnica (conforme as particularidades do sistema criptográfico e/ou de armazenamento de dados estáticos) e juridicamente exigível. Sem essa dupla conformidade não há que se falar em dever fundamental.

Conquanto não seja exigível que provedores enfraqueçam a segurança dos seus sistemas de criptografia, é induvidoso que devem, quando instados pelo Poder Judiciário, prontamente disponibilizar o acesso a dados e comunicações digitais armazenadas em seus servidores e os metadados gerados pelo uso das aplicações.

Não obstante seja consabido que não existem direitos absolutos, sabe-se, igualmente, que o potencial invasivo próprio dos meios de obtenção de prova pode atingir direitos fundamentais. Logo, intervenções estatais sobre o sigilo dos dados telemáticos (comunicacionais ou não) de uma pessoa devem estar respaldos na ordem jurídica vigente, sob pena de responsabilização pessoal e/ou nulificação da prova produzida.

Na vertente das alternativas para a adaptação da persecução penal aos problemas e oportunidades da mensageria criptografada, a análise foi concentrada nos meios de acesso a dados produzidos e armazenados no contexto do uso de aplicações de mensageria pois: (i)

pressupõem a colaboração dos provedores com a entrega dos dados determinada por autoridade judicial; (ii) trata-se de uma das alternativas mais citadas no debate going dark e que está em crescente (porém ainda tímido) uso, (iii) o tema está conectado ao exame de ações de controle abstrato de constitucionalidade com grande potencial de repercussão para o sistema de justiça penal, operadores do direito em geral e toda a sociedade. Talvez colocar a introdução.

Dentre as técnicas processuais à disposição dos órgãos de persecução penal para acesso e registro de dados/evidências digitais, destacam-se as medidas de interceptação do fluxo das comunicações telemáticas e a quebra de sigilo de dados estáticos. Prevista no Marco Civil da Internet, apenas a última possibilita o acesso a dados comunicacionais armazenados em sistemas de nuvens e a metadados gerados nos ambientes das aplicações de mensageria que estejam em repouso nos respectivos servidores/nuvens/data centers.

A mesma intangibilidade que possibilita a mobilidade, disponibilidade e divisibilidade dos dados digitais e que permite o seu armazenamento em data centers em múltiplos lugares do planeta, também atrai o enfrentamento de questões complexas (limites da jurisdição nacional, da soberania e da territorialidade penal na arena virtual) quando as autoridades de persecução se veem em busca de dados armazenados fora do país onde se dá a investigação.

Uma interpretação integrada das normas sobre os direitos e (principalmente) os deveres fundamentais em jogo e de dispositivos da Convenção de Budapeste, do Marco Civil da internet, LINDB e do Código de Processo Civil, sugere que os provedores de serviços de armazenamento remoto de dados que exerçam suas atividades no país devem cumprir prontamente decisões judicias que lhes determine a entrega direta dos dados, sem obrigatoriedade de acionamento da via diplomática pelo uso de cartas rogatórias e acordos MLATs). Ademais, até que sobrevenha decisão da Corte Constitucional Brasileira (na ADC 51) em sentido contrário, todos os dispositivos legais e convencionais criados/incorporados ao ordenamento jurídico interno continuam a gozar de presunção de constitucionalidade das leis, estando aptos à produção de efeitos.

Feitas estas ponderações, cabe retomar o problema principal deste trabalho.

Considerando a essencialidade da criptografia para a concretização de direitos fundamentais, especialmente privacidade e proteção de dados, e ainda os deveres fundamentais dos particulares para com a segurança pública e a administração da justiça, o que pode ser exigido dos provedores de aplicação de mensageria criptografada em relação ao cumprimento de decisões judiciais que determinem a interceptação telemática ou a quebra de sigilo de dados?

Com base no caminho percorrido ao longo dos três capítulos deste trabalho, a resposta ao questionamento pode ser assim sintetizada:

Em relação às interceptações telemáticas, respeitada a arquitetura de cada sistema, tem-se que a criptografia de ponta a ponta inviabiliza a interceptação do fluxo das comunicações, descabendo, consequentemente, sanções por eventuais descumprimentos de decisões judiciais.

Em relação à quebra do sigilo de dados estáticos, os provedores de mensageria criptografada deverão viabilizar pronto e adequado acesso às autoridades de persecução penal aos respectivos dados, metadados ou comunicações digitais armazenadas de que disponham, sempre respeitadas as peculiaridades técnicas da arquitetura de cada sistema.

Vale um alerta final. As cryptowars e o debate going dark deixaram claro que falta de conhecimento técnicos relacionados à arquitetura de sistemas informáticos, aliada à contumaz resistência dos provedores de colaborar com as autoridades rendeu ensejo a quadro endêmico de falta de sinergia entre os atores envolvidos, jogando sobre os ombros da sociedade o produto de uma crise, a provocar a sensação de que onde existir criptografia todas as práticas são permitidas sem que o uso do sistema informativo de alguma forma se volte contra seus usuários maliciosos. A sensação descrita não condiz com a realidade, como se viu. Contudo, a falácia pode se tornar real nos casos em que houver pura e intolerável falta de colaboração voluntária por provedores de aplicações ou se as autoridades de persecução não se capacitarem continua e adequadamente diante dos desafios trazidos pelas inovações tecnológicas ao direito e ao processo penal.

# REFERÊNCIAS

ABELSON, Harold et al. **Chaves embaixo do tapete**: exigências de acesso a todos os dados e comunicações pelo governo geram insegurança. Tradução de R. Sales et al. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio, 2018. Disponível em: https://bit.ly/35Nxuvc. Acesso em: 4 out. 2022.

ABREU, Jacqueline de Souza; ANTONIALLI, Dennys. **Vigilância sobre as comunicações no Brasil**: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais. Internetlab, 2017. Disponível em: http://www.internetlab.org.br/wpcontent/uploads/2017/05/Vigilancia_sobre_as_comunicacoes_no_Brasil_2017_Intern etLab.pdf. Acesso em: 4 out. 2022.

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES (Brasil). **Resolução nº 614, de 28 de maio de 2013**. Brasília, 2013. Disponível em: https://informacoes.anatel.gov.br/legislacao/resolucoes/2013/465-resolucao-614. Acesso em: 4 out. 2022.

AHSAN, Sofi. **After delhi high court ruling, telegram discloses names, phone numbers and ip adresses of users accused of sharing infringing material**. 2022. Disponível em: https://www.livelaw.in/news-updates/after-court-order-telegramdiscloses-phone-numbers-ip-addresses-of-users-accused-of-sharing-infringingmaterial-215311. Acesso em: 30 dez 2022.

ASSEMBLEIA GERAL DA ONU. 2014. Nova York. **O direito à privacidade na era digital**: Relatório do Gabinete do Alto Comissariado das Nações Unidas para os Direitos Humanos. 27ª sessão do Conselho de Direitos. Nova York. 2017. p. 198-199. Disponível em: <https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F27%2F37&Language=E&DeviceType=Desktop&LangRequested=False>. Acesso em: 20 dez. 2022

ALEXY, Robert. Colisão de direitos fundamentais e realização de direitos fundamentais no estado de direito democrático. **Revista de Direito Administrativo**, Rio de Janeiro, n. 217, p. 67-79 jul./set. 1999.

ALIMONTI, Veridiana. Criptografia, direitos e a problemática polarização entre "privacidade individual" e "segurança coletiva". In: DONEDA, Danilo; MACHADO, Diego (Org.). **A criptografia no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2020. E-book.

ALTIERES, Rohr. **Ataque que afetou 74 países usa brecha vazada pelo governo dos EUA**. G1, 12 maio 2017. Disponível em: https://g1.globo.com/tecnologia/blog/seguranca-digital/post/ataque-que-afetou-74paises-usa-brecha-vazada-do-governo-dos-eua.html. Acesso em: 30 abr. 2020.

Apple nega pedido do governo dos EUA para desbloquear iPhones de terrorista. 2020. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2020/01/15/applenega-pedido-do-governo-dos-eua-de-desbloquear-iphones-de-terroristas.htm. Acesso em: 06 out. 2022.

ARANHA, Diego F. O que é criptografia fim a fim e o que devemos fazer a respeito? **Revista dos Tribunais**, Caderno Especial, v. 998, p. 27-40, 2018. Disponível em https://www.researchgate.net/publication/331159816_O_que_e_criptografia_fim-afim_e_o_que_devemos_fazer_a_respeito. Acesso em: 23 ago. 2021. p. 27.

ARENDT, Hannah. **A condição humana**. Tradução de Roberto Raposo. 13. ed. rev. Rio de Janeiro: Forense Universitária, 2020. Livro digital.

ASSEMBLEIA GERAL DA ONU. 2014. Nova York. **O direito à privacidade na era digital**: Relatório do Gabinete do Alto Comissariado das Nações Unidas para os Direitos Humanos. 27ª sessão do Conselho de Direitos. Nova York. 2017. p. 198-199. Disponível em <https://undocs.org/Home/Mobile?FinalSymbol=A%2FHRC%2F27%2F37&Language=E&DeviceType=Desktop&LangRequested=False>. Acesso em: 20 dez. 2022

BARRETO, Alesandro Gonçalves; CASELLI, Guilherme. Exif Metadata - **A investigação policial subsidiada por sua extração e análise**. 2016. Disponível em: https://delegados.com.br/noticia/exif-metadata-a-investigacao-policial-subsidiadapor-sua-extracao-e-analise. Acesso em: 04 out. 2022.

BARROZO, Paulo. **Punição e Constituição**: Cinco Princípios Para o Futuro da Democracia Brasileira (Punishment and the Constitution: Five Principles for the Future of Brazilian Democracy). In: Anais da XXII Conferência Nacional dos Advogados Ordem dos Advogados do Brasil. 2014. p. 6

BELLI, Luca; ZINGALES, Nicolo. **Novas Regras do WhatsApp**: a proteção de dados se torna um luxo para 2 bilhões de pessoas? Disponível em: https://mittechreview.com.br/novas-regras-de-facebook-e-whatsapp-a-protecao-dedados-se-torna-um-luxo-para-2-bilhoes-depessoas/#TB_inline?height=300&width=400&inlineId=single-pdf-download. Acesso em: 20 dez. 2022.

BERKMAN KLEIN CENTER. Don't Panic: **Making progress in the "going dark debate**". Harvard University, 2016. Disponível em: https://itsrio.org/wpcontent/uploads/2018/10/Dont_Panic_Making_Progress_on_Going_Dark_Debate_P T.pdf. Acesso em: 4 out. 2022.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BRANDEIS, Louis; WARREN, Samuel. **The right to privacy**. Harvard Law Review, v. 4, n. 5, p. 193-220, 15 Dec. 1890.

Brasil aprova adesão à Convenção de Budapeste que facilita cooperação internacional para combate ao cibercrime. 2021. Disponível em: https://www.mpf.mp.br/pgr/noticias-pgr/brasil-aprova-adesao-a-convencao-debudapeste-que-facilita-cooperacao-internacional-para-combate-ao-cibercrime. Acesso em: 22 dez. 2022.

BRASIL. Câmara dos Deputados. **Anteprojeto de lei de proteção de dados para segurança pública e persecução penal**. Brasília. Nov. 2020. Disponível em: https://www.conjur.com.br/dl/anteprojeto-lei-disciplina-protecao.pdf. Acesso em: 2 jan. 2023.

BRASIL. Câmara dos Deputados. **Projeto de Lei 10.372, de 2018**. Brasília, 2018. Disponível em: http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=B03D1C179B99D5F4094E807FA8C99F43.proposicoesWebExterno1?codteor=1666497&filename=PL+10372/2018. Acesso em: 31 mar. 2021.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 17 ago. 2021.

BRASIL. **Constituição Política do Imperio do Brazil** (de 25 de março de 1824). Rio de Janeiro, 1824. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao24.htm. Acesso em: 27 ago. 2021.

BRASIL. **Decreto nº 592, de 6 de julho de 1992**. Brasília, 1992. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm. Acesso em: 27 ago. 2021.

BRASIL. **Decreto nº 678, de 6 de novembro de 1992**. Brasília, 1992. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/d0678.htm. Acesso em: 27 ago. 2021.

BRASIL. **Decreto 7.845 de 04 de novembro 2012**. Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento. Brasília. 2012. Disponível em:http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7845.htm. Acesso 02 jan. 2023

BRASIL. **Decreto nº 8.771, de 11 de maio de 2016**. Brasília, 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm. Acesso em: 4 out. 2022.

BRASIL. **Decreto nº. 10.222, de 5 de fevereiro de 2020**. Aprova a Estratégia Nacional de Segurança Cibernética. Brasília, 2020. Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-10.222-de-5-de-fevereiro-de-2020241828419 Acesso em: 03 jan. 2022.

BRASIL. **Decreto nº 10.278, de 18 de março de 2020**. Diário Oficial [da] República Federativa do Brasil, Poder Executivo, Brasília, DF, 19 mar. 2020. Regulamenta o disposto no inciso X do caput do art. 3º da Lei nº 13.874, de 20 de setembro de 2019, e no art. 2º-A da Lei nº 12.682, de 9 de julho de 2012, para estabelecer a técnica e os requisitos para a digitalização de documentos públicos ou privados, a fim de que os documentos digitalizados produzam os mesmos efeitos legais dos documentos originais. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato20192022/2020/decreto/d10278.htm. Acesso em: 26 dez. 2022.

BRASIL. **Decreto nº 19.841, de 22 de outubro de 1945**. Brasília, 1945. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1930-1949/d19841.htm. Acesso em: 27 ago. 2021.

BRASIL. **Decreto Legislativo nº 37 de dezembro de 2021**. Aprova o texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001. Brasília, 2001.

BRASIL. **Decreto-lei nº 3.689, de 3 de outubro de 1941**. Brasília, 1941. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 22 dez. 2022.

BRASIL. **Decreto-Lei nº 3.810, de 2 de maio de 2001**. Brasília, 2001. Disponível em: https://legis.senado.leg.br/norma/402272#:~:text=PROMULGA%20O%20ACORDO%20DE%20ASSISTENCIA,EM%2015%20DE%20FEVEREIRO%202001. Acesso em: 22 dez. 2022.

BRASIL. **Decreto-Lei nº 4.657, de 4 de setembro de 1942**. Brasília, 1942. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del4657.htm. Acesso em: 10 dez. 2022.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996**. Brasília, 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em: 6 out. 2022.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Brasília, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 1º ago. 2021.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Brasília, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm#:~:text=O%20provedor%20de%20aplica%C3%A7%C3%B5es%20de,prazo%20de%206%20(seis)%20meses. Acesso em: 1º ago. 2021.

BRASIL. **Lei nº 13.105, de 16 de março de 2015**. Brasília, 2015. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 22 dez. 2022.

BRASIL. **Lei nº 13.709, de 13 de agosto de 2018**. Brasília, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 1º ago. 2021.

BRASIL. **Lei nº 13.964, de 24 de dezembro de 2019**. Brasília, 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13964.htm. Acesso em: 22 dez. 2022.

BRASIL. **Medida Provisória nº 954, de 2020**. Brasília, 2020. Disponível em: https://www.congressonacional.leg.br/materias/medidas-provisorias/-/mpv/141619. Acesso em: 22 dez. 2022.

BRASIL. **Ministério da Justiça e Segurança Pública**. Declaração do Going Dark Brasil. Brasília, 12 fev. 2019. Disponível em:

https://www.justica.gov.br/news/collective-nitf-content-1550010028.2/documentos/declaracao-do-going-dark-brasil.pdf. Acesso em: 7 out. 2022. p. 1.

BRASIL. Ministério da Justiça e Segurança Pública. **MJSP promove simpósio internacional sobre "Going Dark"**. Brasília, 8 fev. 2019. Disponível em: https://www.justica.gov.br/news/collective-nitf-content-1549651780.89. Acesso em: 7 out. 2022.

BRASIL. Superior Tribunal de Justiça. **Além de multa, empresas de tecnologia que não fornecem dados à Justiça podem ter valores bloqueados e nome inscrito em dívida ativa**. Brasília, 01 jul. 2020. Disponível em:https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/Alem-de-multa-empresas-de-tecnologia-que-nao-fornecem-dados-a-Justica-podem-ter-valoresbloqueados-e-nome-inscrito-em-divi.aspx. Acesso em: 3 ago. 2022.

BRASIL. Superior Tribunal de Justiça. **Criptografia em aplicativo de mensagem não permite multa cominatória, decide Quinta Turma**. Brasília, 24 jun. 2021. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/24062021Criptografia-em-aplicativo-de-mensagem-nao-permite-multa-cominatoria--decideQuinta-Turma.aspx. Acesso em: 3 ago. 2022.

BRASIL. Superior Tribunal de Justiça. **EDcl no AgRg no RMS n. 63.492/AC**. Relator Ministro Ribeiro Dantas, Quinta Turma, julgado em 17/11/2020, Brasília, DJe de 23/11/2020.)

BRASIL. Superior Tribunal de Justiça. **Recurso em Habeas Corpus nº 99.735**. Relatora Ministra Laurita Vaz. Brasília, 2018. Disponível em: http://www.internetlab.org.br/wp-content/uploads/2018/12/document.pdf. Acesso em: 31 set. 2022.

BRASIL. Superior Tribunal de Justiça. **Recurso em Mandado de Segurança nº 66.392 RS**. (2021/0134439-7). Recorrente: FI. Recorrido: Ministério Público Federal. Relator: Ministro João Otávio De Noronha. DJ 16 ago. 2022. Disponível em: https://processo.stj.jus.br/processo/julgamento/eletronico/documento/mediado/?documento_tipo=integra&documento_sequencial=162042498&registro_numero=202101344397&peticao_numero=&publicacao_data=20220819&formato=PDF. Acesso em 18 nov. 2022.

BRASIL. Superior Tribunal de Justiça. **Recurso Ordinário em Mandado de Segurança 60.531/RO**. Recorrente: WhatsApp Inc. Recorrido: Ministério Público de Rondônia Rel. Ministro Nefi Cordeiro, Rel. Acórdão: Ministro Ribeiro Dantas, Terceira Seção, julgado em 09/12/2020, DJe 17/12/2020

BRASIL. Superior Tribunal de Justiça. **Terceira Seção afasta multa contra empresa que alega impossibilidade de interceptar mensagens criptografadas**. Brasília, 30 dez. 2020. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/30122020Terceira-Secao-afasta-multa-contra-empresa-que-alega-impossibilidadedeinterceptar-mensagens-criptografadas.aspx. Acesso em: 3 ago. 2022.

BRASIL. Supremo Tribunal Federal. **Ação Declaratória de Constitucionalidade nº 51**. Brasília, 2022. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=5320379. Acesso em: 22 dez. 2022.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade 5.527**. Marco Civil da internet. Relatora: Ministra Rosa Weber. Arguição de Descumprimento de Preceito Fundamental403. Bloqueio judicial do whatsapp. Relator: Ministro Edson Fachin. Transcrição da audiência pública. p. 48-50 Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/Alem-demulta--empresas-de-tecnologia-que-nao-fornecem-dados-a-Justica-podem-tervalores-bloqueados-e-nome-inscrito-em-divi.aspx. Acesso em: 02 jan. 2023

BRASIL. Supremo Tribunal Federal. **Audiência pública – controle de dados de usuários por provedores de Internet no exterior (1/2)**. Brasília, 12 fev. 2020. Disponível em: https://www.youtube.com/watch?v=x6nMFtg70FE (a partir de 1h16). Acesso em: 4 out. 2022.

BRASIL. Supremo Tribunal Federal. **Arguição de Descumprimento de Preceito Fundamental nº 403 Sergipe**. Relator Ministro Edson Fachin. Brasília, 2020. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stf/853369813. Acesso em: 22 dez. 2022.

BRASIL. Supremo Tribunal Federal. Edital de convocação conjunta de audiência pública. **Ação Direta de Inconstitucionalidade nº 5.527**. Brasília, 29 nov. 2016. Disponível em: https://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/adpf403.pdf. Acesso em: 9 out. 2022.

BRASIL. Supremo Tribunal Federal. **Petição 9.935 Distrito Federal**. Relator Ministro Alexandre de Moraes. Brasília, 2001. Disponível em: https://www.conjur.com.br/dl/alexandre-moraes-ordena-bloqueio.pdf. Acesso em: 22 dez. 2022.

BRASIL. Supremo Tribunal Federal. **Referendo na medida cautelar na Ação Direta de Inconstitucionalidade 6.387 Distrito Federal**. Requerente: Conselho Federal da Ordem dos Advogados do Brasil (CFOAB). Relatora: Min. Rosa Weber. DJE 11/11/2020. Disponível em: http://portal.stf.jus.br/processos/detalhe.asp?incidente=5895165. Acesso em: 23 ago. 2021.

BRASIL. Supremo Tribunal Federal. Segunda Turma. **Recurso Ordinário em Habeas Corpus 132.115**. Relator: Min. Dias Toffoli, julg. 6.2.2018, processo eletrônico, DJe 223, divulg. 18.10.2018, public. 19 out. 2018

BRASIL. Supremo Tribunal Federal. Tribunal Pleno. **Mandado de Segurança nº 23452/RJ**. Comissão Parlamentar de Inquérito. Poderes de investigação. limitações constitucionais. legitimidade do controle jurisdicional. Possibilidade de a CPI ordenar, por autoridade própria, a quebra dos sigilos bancário, fiscal e telefônico. Necessidade de fundamentação do ato deliberativo. Deliberação da CPI quem sem fundamentação, ordenou medidas de restrição a direitos. Mandado de Segurança deferido. Impetrante: Luiz Carlos Barretti Júnior. Impetrado: Presidente da Comissão Parlamentar de Inquérito. Relator:.Ministro Celso de Mello. Data da Decisão: 16 de set. 1999

BUARQUE, Rodrigo Costa; PEDRA, Adriano Sant'Ana. A recusa das partes à audiência preliminar no novo código de processo civil: necessidade de motivação ante o dever fundamental de cooperação com a justiça. **Revista Magister de Direito Civil e Processual Civil**, Porto Alegre, n. 72, p. 112-123, maio/jun. 2016.

BVerfGE 65, 1, "Recenseamento" (Volkszählung). MARTINS, Leonardo (Org.) **Cinquenta anos de Jurisprudência do Tribunal Constitucional federal alemão**. Montevidéu: Fundação Konrad Adenauer, 2005.

CAMPOS, Luiz Fernando de Barros. Metadados digitais: revisão bibliográfica da evolução e tendências por meio de categorias funcionais. **Encontros Bibli: Revista Eletrônica de Biblioteconomia e Ciência da Informação**, [S. l.], v. 12, n. 23, p. 17, 2007. DOI: 10.5007/1518-2924.2007v12n23p16. Disponível em: https://periodicos.ufsc.br/index.php/eb/article/view/1518-2924.2007v12n23p16. Acesso em: 11 jan. 2023.

CARDOSO, Jessica; SCHNEIDER, Victor. **Telegram já foi bloqueado ou restringido em 11 países**. Poder 360, 14 fev. 2022. Disponível em: https://www.poder360.com.br/internacional/telegram-ja-foi-bloqueado-ou-restringidoem-11-paises-leia-quais/. Acesso em: 22 dez. 2022.

CASALTA NABAIS, José. **O dever fundamental de pagar impostos**: contributo para a compreensão constitucional do estado fiscal contemporâneo. Coimbra: Almedina. 2002.

CASTRO, Daniel; MCQUINN, Alan. **Unlocking Encryption**: Information Security and the Rule of Law. Information Technology & Innovation Foundation, 2016. Disponível em: https://www2.itif.org/2016-unlocking-encryption-exec-summary.pdf. Acesso em: 4 out. 2022.

COLNAGO, Claudio de Oliveira Santos. Provedores de conexão e guarda de registros de acesso a aplicações de Internet: o art. 14 do Marco Civil no contexto do dever fundamental de preservação do meio ambiente digital. In: George Salomão Leite, Ronaldo Lemos. (Org.). **Marco Civil da Internet**. São Paulo: Atlas, 2014, v. 1, p. 755-771.

COLNAGO, Claudio de Oliveira Santos; PEDRA, Adriano Sant'Ana. Meio ambiente digital, arquitetura e direito de resposta: os deveres dos prestadores de serviços de internet. In: BAEZ, Narciso L. X.; STURMA, Pavel; MOZETIC, Vinicius A.; FAIX, Martin. (Org.). **Mecanismos internacionais e internos de efetividade dos direitos fundamentais**. Chapeço: Editora Unoesc, 2014, v. 1, p. 397-419. p. 398.

COMEY, James. **Going Dark**: Are Technology, Privacy, and Public Safety on a Collision Course? Washington: Brooklings Institution, 2014. Disponível em: https://bit.ly/32DztQN. Acesso em: 2 out. 2022.

COMO funciona o app 'ultrasseguro' de mensagens usado por Snowden. 2016. Disponível em: https://www.bbc.com/portuguese/geral-37821449. Acesso em: 18 mar. 2022.

CORRÊA. Rodrigo Henrique Luiz. **Big Data e Criptografia**: o lugar do direito Fundamental à privacidade diante das novas tecnologias da informação e comunicação big data e criptografia. 2018. Mestrado em Direito Civil Constitucional; Direito da Cidade; Direito

Internacional e Integração Econômica. Universidade do Estado do Rio de Janeiro, Rio de Janeiro. Data de aprovação: 21 de maio de 2018.

COSSETTI, Melissa Cruz. **O que são dados EXIF de fotos**: em cada foto, a câmera ou o celular gera e registra dados exif sobre como, quando e onde a imagem foi registrada. Em cada foto, a câmera ou o celular gera e registra dados EXIF sobre como, quando e onde a imagem foi registrada. 2019. Disponível em: https://tecnoblog.net/responde/o-que-sao-dados-exif-de-fotos-e-como-encontra-losou-esconde-los/. Acesso em: 04 out. 2022,

COSTA, Diogo Erthal Alves da. Nemo tenetur se detegere e dados criptografados: restabelecendo o equilíbrio. In: SALGADO, Daniel Resende; QUEIROZ, Ronaldo Pinheiro de (org.). **A prova no enfrentamento à macrocriminalidade**. São Paulo: JusPodivm, 2019. p. 209-252.

DASKAL, Jennifer C. The Un-Territoriality of Data. **125 Yale Law Journal**, American University, WCL Research Paper, n. 2015-5, 2015. Disponível em: https://ssrn.com/abstract=2578229. Acesso em: 10 dez. 2022.

DE SOUZA ABREU, Jacqueline. Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação. **Revista Brasileira de Políticas Públicas**, v. 7, n. 3, p. 24-42, 2017.

DIFFIE, Whitfield; LANDAU; Susan. **Privacy on the line**: the politics of wiretapping and encryption. Cambridge: The MIT Press, 2007.

DOMINGOS, Fernanda Teixeira Souza; RÖDER, Priscila Costa Schreiner. Obtenção de provas digitais e jurisdição na Internet. Escola de Magistrados da Justiça Federal da 3ª Região. **Caderno de Estudos, Investigação e Prova nos Crimes Cibernéticos**, São Paulo, v. 1, p. 55-84, 2017. Disponível em: https://memorial.mpf.mp.br/nacional/vitrine-virtual/publicacoes/crimes-ciberneticoscoletanea-de-artigos. Acesso em: 10 dez. 2022.

DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2. ed. São Paulo: Thomson Reuters Brasil, 2020. Livro digital.

DONEDA, Danilo; MACHADO, Diego. **A criptografia no Direito brasileiro**. Edição do Kindle. Thomson Reuters, Revista dos Tribunais, 2019.

DUAN, Charles et al. **Policy Approaches to the Encryption Debate**. Policy Paper. R Street Policy Study, n. 133, 2018. Disponível em: http://2o9ub0417chl2lg6m43em6psi2i.wpengine.netdna-cdn.com/wpcontent/uploads/2018/03/133.pdf. Acesso em: 4 out. 2022.

FABRIZ, Daury Cesar; GONÇALVES, Luísa Cortat Simonetti. Dever fundamental: a construção de um conceito. In: DE MARCO, Cristhian Magnus; PEZZELLA, Maria Cristina Cereser; STEINMETZ, Wilson (org.). **Teoria geral e mecanismos de efetividade no Brasil e na Espanha**: Série Direitos Fundamentais Civis. Joaçaba: Unoesc, 2013. tomo I. p. 87-96.

FABRIZ, Daury Cesar; LARANJA, Anselmo Laghi; PEDRA, Adriano Sant'Ana. Diferenças e semelhanças na positivação de deveres fundamentais no constitucionalismo espanhol e brasileiro: diálogo entre Francisco Rubio Llorente e o Grupo de Pesquisa "Estado, Democracia e Direitos Fundamentais". Constituição, Economia e Desenvolvimento: **Revista da Academia Brasileira de Direito Constitucional**, Curitiba, 2020, v. 11, n. 21, p. 263-297, ago./dez. 2019.

FACEBOOK, Google e WhatsApp planejam aumentar criptografia de dados de usuários: estimulados pelas batalhas da Apple contra o FBI, alguns dos maiores nomes da tecnologia estão expandindo a criptografia de dados do usuário em seus serviços, o Guardian pode revelar. Estimulados pelas batalhas da Apple contra o FBI, alguns dos maiores nomes da tecnologia estão expandindo a criptografia de dados do usuário em seus serviços, o Guardian pode revelar. 2017. Disponível em: https://www.theguardian.com/technology/2016/mar/14/facebook-google-whatsappplan-increase-encryption-fbi-apple. Acesso em: 06 out. 2022.

FBI não dirá à Apple como conseguiu desbloquear iPhone de atirador: polícia federal dos eua recorreu a hackers após apple se negar a ajudar. FBIconseguiu acesso a celular de atirador que matou 14 na Califórnia. Polícia federal dos EUA recorreu a hackers após Apple se negar a ajudar. FBI conseguiu acesso a celular de atirador que matou 14 na Califórnia. 2016. Disponível em: https://g1.globo.com/tecnologia/noticia/2016/04/fbi-nao-dira-apple-como-conseguiudesbloquear-iphone-de-atirador.html. Acesso em: 06 out. 2022.

FERNANDES, Antônio Scarance. O polêmico inciso XII do Art. 5º da Constituição Federal. **Justitia**, São Paulo, 64, jul-dez. 2007, p. 17 e 21.

FIGUEIREDO JUNIOR, Jorge; PATURY, Fabrício Rabelo. Quebra telemática de whatsapp e sua utilização no combate ao crime organizado. In: PAULINO, Galtiênio da Cruz, et al. Técnicas avançadas de investigação. Brasília: ESMPU, 2022. 2º volume. p. 283-290. p. 286.

FISCHER, Douglas. **Influências principiológicas da Constituição da República e do novo CPC no processo penal**. Salvador: Juspodivm, 2016. v. 13. Coleção repercussões do novo CPC: processo penal.

FRANCO, Marcela. Qual é a origem do Telegram? Veja curiosidades sobre o polêmico app russo. **TechTudo**, 22 mar. 2022. Disponível em: https://www.techtudo.com.br/listas/2022/03/qual-e-a-origem-do-telegram-vejacuriosidades-sobre-o-polemico-app-russo.ghtml. Acesso em: 22 dez. 2022.

FREIRE JÚNIOR, Américo Bedê. **A retórica do direito fundamental à privacidade**: A validade da prova obtida mediante filmagens nos ambientes públicos e privado. Salvador: JusPodivm, 2015.

FREIRE JÚNIOR, Américo Bedê; SENNA, Gustavo. **Princípios do processo penal**: entre o garantismo e a efetividade da sanção. São Paulo: Revista dos Tribunais, 2009.

GILL, Lex; ISRAEL, Tamir; PARSONS, Christopher. **Shining a Light on the Encryption Debate**: a Canadian field guide. CitizenLab, University of Toronto, 2018. Disponível em: https://citizenlab.ca/wp-content/uploads/2018/05/Shining-A-LightEncryption-CitLab-CIPPIC.pdf. Acesso em: 4 out. 2022.

GLEIZER, Orlandino; MONTENEGRO, Lucas; VIANA, Eduardo. **O direito de proteção de dados no processo penal e na segurança pública**. São Paulo: Marcial Pons, 2021. p. 121 e 124).

GREENWALD, Glenn et al. Como e por que o Intercept está publicando chats privados sobre a Lava Jato e Sergio Moro. **The Intercept**, 9 jun. 2019. Disponível em: https://theintercept.com/series/mensagens-lava-jato/. Acesso em: 9 out. 2022.

GRESCHBACH, Benjamin; KREITZ, Gunnar; BUCHEGGER, Sonja. The devil is in the metadata— New privacy challenges in Decentralised Online Social Networks. In: **Pervasive Computing and Communications Workshops (PERCOM Workshops)**, 2012, Lugano. p. 333-339. Disponível em: https://ieeexplore.ieee.org/document/6197506. Acesso em: 16 abr. 2022

GRINOVER, Ada Pellegrini. O regime brasileiro das interceptações telefônicas. **Revista Brasileira de Ciências Criminais**, São Paulo, n. 17, p. 112-126, jan.-mar. 1997.

GROBÉRIO, Sonia do Carmo. PEDRA, Adriano Sant'Ana. Segurança Pública como responsabilidade de todos: análise à luz da teoria dos deveres fundamentais da das políticas públicas de segurança. **Revista Paradigma**, Ribeirão Preto, a. XXVII, v. 31, n. 1, p. 217-239 jan/abr 2022

HABERMAS, Jürgen. **Mudança estrutural da esfera pública**: investigações sobre uma categoria da sociedade burguesa. Tradução de Flávio R. Kothe. Rio de Janeiro: Tempo Brasileiro, 2003.

HEATH, Brad. **FBI warned agents not to share tech secrets with prosecutors**. 2016. Disponível em: https://www.usatoday.com/story/news/2016/04/20/fbi-memossurveillance-secrecy/83280968/. Acesso em: 31 dez. 2022.

HOFFMANN-RIEM, Wolfgang. Autorregulação, autorregulamentação e autorregulamentação regulamentada no contexto digital. **Revista da Ajuris**, v. 46, n. 146, p. 529-554, 2019.

HOFFMANN-RIEM. **Teoria geral do direito digital**. Edição do Kindle. Forense, 2022.

INVESTIGAÇÃO de morte de juíza fecha o cerco sobre policiais acusados de crimes. Veja. 2011. Disponível em: <https://veja.abril.com.br/brasil/investigacao-de-morte-dejuiza-fecha-o-cerco-sobre-policiais-acusados-de-crimes/>; e Justiça mantém penas de seis PMs envolvidos na morte de juíza no Rio. Folha de S. Paulo. 2016. Disponível em: https://www1.folha.uol.com.br/cotidiano/2016/10/1820061-justicamantem-penas-de-seis-pms-envolvidos-na-morte-de-juiza-no-rio.shtml. Acesso em: 31 dez de 2022.

JOHN SNOW. Signal é seguro. **Quem comprova são os hackers**. 2022. Disponível em https://www.kaspersky.com.br/blog/signal-hacked-but-still-secure/19942/. Acesso em: 31 dez. 2022.

JORGE, Higor Vinicius Nogueira; FONSECA, Ricardo Magno Teixeira. Fraudes com o auxílio da tecnologia e relevância da investigação criminal tecnológica. In: VERGINE,

Gaetano; JORGE, Higor Vinicius Nogueira. **Relatos sobre a investigação de crimes cibernéticos**. Salvador: Juspodivm, 2022. p. 147 a 162. Disponível em: https://www.editorajuspodivm.com.br/relatos-sobre-a-investigacao-de-crimesciberneticos-2022. Acesso em: 02 jan 2023.

KROLL, Andy. **Documento do FBI diz que os federais podem obter seus dados do WhatsApp em tempo real**. 2021. Disponível em: <https://www.rollingstone.com/politics/politics-features/whatsapp-imessagefacebook-apple-fbi-privacy-1261816/> Acesso em: 31 de dez de 2022

KUEHN, Andreas; MCCONNELL, Bruce. **Encryption Policy in Democratic Regimes**: Finding Convergent Paths and Balanced Solutions. EastWest Institute, 2018. Disponível em: https://www.eastwest.ngo/sites/default/files/ewi-encryption.pdf. Acesso em: 4 out. 2022.

LAFER, Celso. **A reconstrução dos direitos humanos**: um diálogo com o pensamento de Hannah Arendt. São Paulo: Companhia das Letras, 1988.

LEE, Micah. **Batalha dos aplicativos de mensagens seguras**: como o Signal supera o Whatsapp. 2016. Disponível em: https://theintercept.com/2016/06/22/battle-of-the-secure-messaging-apps-how-signalbeats-whatsapp/. Acesso em: 31 dez. 2022.

LEONARDI, Marcel. **Tutela e privacidade na internet**. Imprenta: São Paulo, Saraiva, 2012.

LEWIS, James; ZHENG, Denise; CARTER, William. **The Effect of Encryption on Lawful Access to Communications and Data**. Center for Strategic & International Studies, 2017. Disponível em: https://csis-website-prod.s3.amazonaws.com/s3fspublic/publication/170221_Lewis_EncryptionsEffect_Web.pdf. Acesso em: 4 out. 2022.

LIGUORI, Carlos. **Direito e criptografia**: direitos fundamentais, segurança da informação e os limites da regulação jurídica na tecnologia. São Paulo: Saraiva Jur, 2022.

LIGUORI, Carlos; SALVADOR, João Pedro. Crypto wars e bloqueio de aplicativos: o debate sobre regulação jurídica da criptografia nos Estados Unidos e no Brasil. **Revista da Faculdade de Direito da UFPR**, Curitiba, v. 63, n. 3, p. 135-161, set./dez. 2018. Disponível em: https://revistas.ufpr.br/direito/article/view/59422. Acesso em: 22 dez. 2018.

LINHARES, Rafael Lima. O uso de kdd e de red flags para o enfrentamento das organizações criminosas e para a criação de matrizes de risco na lavagem de capitais. In: PAULINO, Galtienio da Cruz, et al. **Técnicas avançadas de investigação**. Brasília: ESMPU, 2022, p. 177.

MACASKILL, E. et al. NSA files decoded: Edward Snowden's surveillance revelations explained. **The Guardian**, 1º nov. 2013. Disponível em: https://goo.gl/MEmVl5. Acesso em: 6 out. 2022.

MALINOWSKI, Carlos Eduardo. Capítulo V– Direitos Humanos Frente à Revolução Tecnológica: implicações sociológicas e jurídicas. In: SUNAKOZAWA, Lúcio Flavio Joichi;

FURLANI, Carlos Eduardo Pereira; BRILTES, Aurélio Tomaz da Silva; SILVA, Ludmila de Paula Castro. **Direito do Estado e suas novas dimensões no terceiro milênio**: Estado e jurisdição, políticas públicas e sustentabilidade: estudos em homenagem ao professor Olyntho Luiz Cestari Mancini. Campo Grande: ALJ-MS, 2020. p. 46-86.

MARIN, Jorge. **Tweet de Elon Musk faz acesso ao Signal viralizar**. 2021. Disponível em: https://www.tecmundo.com.br/internet/209107-tweet-elon-muskacesso-signal viralizar.htm#:~:text=Use%20Signal%2C%20segundo%20a%20l%C3%ADngua,%2C %20em%20mais%20de%20500%25. Acesso em: 28 dez. 2022.

MCCLURE, Stuart; SCAMBRAY, Joel; KURTZ, George. **Hackers expostos**: segredos e soluções para a segurança de redes. 7. ed. Tradução de João Eduardo Nóbrega Tortello. Porto Alegre: Bookman, 2014.

MCCONNELL, Mike; CHERTOFF, Michael; LYNN, William. Why the fear of ubiquitous data encryption is overblown. **The Washington Post**, 28 jul. 2015.

MENDES, Laura Schertel. **Autodeterminação informativa**: a história de um conceito. No prelo.

MITCHELL, Bonnie et al. **Going Dark**: Impact to Intelligence and Law Enforcement and Threat Mitigation. 2017. Disponível em: https://cyberwar.nl/d/fromDNI.gov/10--2017-AEP_Going-Dark.pdf. Acesso em: 31 set. 2022.

MOBILE TIME; OPINION BOX. **Panorama Mobile Time/Opinion Box**: mensageria no Brasil. Ago. 2022. Disponível em: https://www.mobiletime.com.br/pesquisas/mensageria-no-brasil-agosto-de-2022/. Acesso em: 22 out. 2022.

MORAES, Maria Celina Bodin de. Rodotà. **Blog Teoria do Direito Privado**, 28 jan. 2016. Disponível em: http://teoriadodireitoprivado.blogspot.com/2016/01/rodota.html. Acesso em: 17 ago. 2021.

MORAIS, José Luis Bolzan de. O Estado de Direito "confrontado" pela "Revolução da Internet". Revista Eletrônica do Curso de Direito da UFSM, v. 13, n. 3, p. 876-903, 2018.

MORAIS, José Luis Bolzan de. LOBO, Edilene. **Temas de Estado de direito e tecnologia**. Porto Alegre: Fi, 2021.

MULLER, Leo. MPF investiga possível inconstitucionalidade da criptografia do Whatsapp. **Tecmundo**, 6 maio 2016. Disponível em: https://www.tecmundo.com.br/whatsapp/104522-mpf-investida-possivelinconstitucionalidade-criptografia-whatsapp.htm. Acesso em: 4 out. 2022.

NATIONAL ACADEMIES OF SCIENCES, ENGINEERING & MEDICINE. **Decrypting the Encryption Debate**: A framework for decision makers. Washington: The National Academies Press, 2018. p. 6.

Noções básicas de metadados. **Dublincore** [s.d.]. Disponível em: https://www.dublincore.org/resources/metadata-basics/ Acesso em: 8 jan. 2023

O que é criptografia pós-quântica? A corrida para criar novas formas de proteger os dados e as comunicações da ameaça representada por computadores quânticos superpoderosos já começou. 2020. Disponível em: https://mittechreview.com.br/oque-e-criptografia-pos-quantica/. Acesso em: 2 jan. 2023.

O que é um ataque de força bruta? ataques de força bruta quebram a segurança dos dados ao tentar todas as combinações possíveis, como um ladrão que invade um cofre testando todos os números para abrir a fechadura. Disponível em: https://www.cloudflare.com/pt-br/learning/bots/brute-force-attack/. Acesso em: 3 jan. 2023.

O que é um computador quântico? Como funciona, por que é tão poderoso e onde, a princípio, é provável que seja mais útil. 2020. Disponível em: https://mittechreview.com.br/o-que-e-um-computador-quantico/ Acesso em 2 jan. 2023.

O que são Metadados? Metadados, [s.d.]. Disponível em: http://www.metadados.pt/oquesaometadados/. Acesso em: 11 dez. 2022

PADRÃO, Marcio. **Caso Marielle**: como celulares levaram a acusados e por que isso é um avanço. UOL. 2019. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2019/03/13/como-os-celularesajudaram-a-achar-o-assassino-de-marielle-franco.htm. Acesso em: 31 de dez. de 2022.

PEDRA, Adriano Sant'Ana. **A Constituição viva**: poder constituinte permanente e cláusulas pétreas na democracia participativa. 5. ed. Rio de Janeiro: Lumen Juris, 2018.

PEDRA, Adriano Sant'Ana. A importância dos deveres humanos na efetivação de direitos. In: Robert Alexy et al. (org.). **Níveis de efetivação dos direitos fundamentais civis e sociais**: um diálogo Brasil e Alemanha. Joaçaba: Unoesc, 2013. p. 281-301.

PEDRA, Adriano Sant'Ana. As diversas perspectivas dos direitos fundamentais. **Revista de Direitos e Garantias Fundamentais**, Vitória, v. 18, n. 2, p. 9-12, 9 fev. 2018.

PEDROSA, Paulo H. C.; NOGUEIRA, Thiago. **Computação em nuvem**. Unicamp, 2011. Disponível em: https://www.ic.unicamp.br/~ducatte/mo401/1s2011/T2/Artigos/G04-095352-120531t2.pdf. Acesso em: 29 nov. 2022.

PEREIRA, Ana Bárbara Gomes; RODRIGUES, Gustavo Ramos; VIEIRA, Victor Barbieri Rodrigues. **Percepções sobre criptografia e investigações criminais no Brasil**: mapeamento e análise. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2021. Disponível em: https://bit.ly/3kGTde3. Acesso em: 4 out. 2022.

PEZZOTTI, Olavo Evangelista. Interceptação telemática, quebra de sigilo de dados e a resistência das big techs: alternativas disponíveis aos órgãos de persecução penal e ao Poder Judiciário. In: PAULINO, Galtiênio da Cruz et al. (Org.). **Técnicas avançadas de investigação**. Brasília: ESMPU, 2022. p. 237-281.

QUEIROZ, Rafael Mafei Rabelo. Privacidade, criptografia e dever de cumprimento de ordens judiciais por aplicativos de troca de mensagens. In: DONEDA, Danilo; MACHADO, Diego.

**A criptografia no Direito brasileiro**. Edição do Kindle. Thomson Reuters, Revista dos Tribunais, 2019.

RAZERA, Gustavo Eloi. Acesso a dados criptografados no contexto de investigações criminais: o "estado da arte". **Revista do Ministério Público do Estado do Rio de Janeiro**, n. 79, p. 143-165, jan./mar. 2021.

ROCHA, Marcelo. Telegram mantém representante no Brasil há 7 anos enquanto ignora STF e TSE. **Folha de São Paulo**, São Paulo, 19 fev. 2022. Disponível em: https://www1.folha.uol.com.br/poder/2022/02/telegram-mantem-representante-nobrasil-ha-7-anos-enquanto-ignora-stf-e-tse.shtml. Acesso em: 12 mar. 2022.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Tradução de Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SAMPAIO, José Adércio Leite. Comentário ao art. 5º, inciso X. In: CANOTILHO, J. J. Gomes et al. (Coords.). Comentários à Constituição do Brasil. São Paulo: Saraiva/Almedina, 2013. Livro digital.

SAMPAIO, José Adércio Leite. **Direito à intimidade e à vida privada**. Belo Horizonte: Del Rey, 1998.

SANTOS, Marcelo; FAURE, Antoine. Programar é poder: contradições entre as dimensões comunicacional e tecnológica da criptografia de ponta a ponta. **Revista Interamericana de Comunicação Midiática**, Rio Grande do Sul, v. 18, n. 36, p. 5885, maio 2019.

SCHULZ, Wolfgang; VAN HOBOKEN, Joris. **Human Rights and Encryption**. UNESCO Series on Internet Freedom, 2016. Disponível em: https://www.gcedclearinghouse.org/sites/default/files/resources/170056eng.pdf. Acesso em: 8 jun. 2021.

SILVA, José Afonso da. **Curso de direito constitucional positivo**. 37. ed. São Paulo: Malheiros, 2009.

SIGNAL: entenda por que o aplicativo de mensagens é considerado ultrasseguro. 2019. Disponível em: <https://www.estadao.com.br/link/signal-entenda-por-que-oaplicativo-de-mensagens-e-considerado-ultrasseguro/>. Acesso em: 31 de dez de 2022.

STALLINGS, William. **Criptografia e segurança de redes**: princípios e práticas. Tradução de Daniel Vieira. 6. ed. São Paulo: Pearson Education do Brasil, 2015.

SUNAKOZAWA, Lúcio Flavio Joichi et al. **Direito do Estado e suas novas dimensões no terceiro milênio**: Estado e jurisdição, políticas públicas e sustentabilidade. Estudos em homenagem ao professor Olyntho Luiz Cestari Mancini. Campo Grande: Academia de Letras Jurídicas do Estado de Mato Grosso do Sul, 2020.

SWIRE, Peter; AHMAD, Kenesa. Encryption and Globalization. **The Columbia Science & Technology Law Review**, v. 13, p. 416-481, 2012.

SWIRE, Peter; HEMMINGS, Justin D.; VERGNOLLIE, Suzanne. A Mutual Legal Assistance Case Study: The United States and France. Hal open science. **Lyon**, v. 34, p. 102-144, 2016

TATUM, Malcolm. **What is a pen register**? dezembro de 2022. Disponível em < https://www.easytechjunkie.com/what-is-a-pen-register.htm> Acesso em: 21 de dez. 2022

TAVARES, André Ramos. **Curso de direito constitucional**. 4. ed. São Paulo: Saraiva, 2006.

TEIXEIRA, Tarcisio; SABO, Paulo Henrique; SABO, Isabela Cristina. Whatsapp e a criptografia ponto-a-ponto: tendência jurídica e o conflito privacidade vs. interesse público. **Revista da Faculdade de Direito da UFMG**, Belo Horizonte, n. 71, p. 607638, jul./dez. 2017.

VALVERDE, Danielle Novaes de Siqueira. **Evidências criminais eletrônicas em nuvem e sua coleta extraterritorial no processo penal**. 2018. 292 f. Tese (Doutorado) – Programa de Pós-Graduação em Ciência da Computação, Universidade Federal de Pernambuco, Recife, 2018.

VELLO, Renata Pinto Coelho; PEDRA, Adriano Sant'Ana. O dever fundamental de testemunhar: uma análise de sua eficácia horizontal. In: BUSSINGUER, Elda Coelho de Azevedo (org.). **Direitos fundamentais**: pesquisas. Curitiba: CRV, 2011. p. 193-199.

VITAL, Danilo. Telegram cumpre ordens judiciais, e Alexandre determina desbloqueio. **Revista Consultor Jurídico**, 20 mar. 2022. Disponível em: https://www.conjur.com.br/2022-mar-20/telegram-cumpre-ordens-judiciais-alexandredetermina-desbloqueio. Acesso em: 22 dez. 2022.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. Interceptação telemática de contas do whatsapp (bilhetagem - extrato de mensagens. In: JORGE, Higor Vinicius Nogueira. **Tratado de investigação criminal tecnológica**. 2. ed. Salvador, Juspodivm, 2021, p. 139-147.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância**: a luta por um futuro humano na nova fronteira do poder. Rio de Janeiro: Intrínseca, 2019a. Livro digital.

ZUBOFF, Shoshana. **Um capitalismo de vigilância**. Le monde diplomatique Brasil, São Paulo, 3 jan. 2019b. Disponível em: https://diplomatique.org.br/um-capitalismo-de-vigilancia/. Acesso em: 4 jul. 2021.