O DIREITO DAS INVESTIGAÇÕES DIGITAIS NO BRASIL ////// FUNDAMENTOS E MARCOS NORMATIVOS

São Paulo, agosto de 2022

< 3. EDIÇÃO >

INTERNETLAB
pesquisa em direito e tecnologia

O InternetLab é uma organização sem fins lucrativos dedicada à produção de pesquisa acadêmica aplicada com impacto em políticas públicas de tecnologia e Internet no Brasil.

Citação sugerida
INTERNETLAB. O direito das investigações digitais no Brasil: fundamentos e marcos normativos. São Paulo: InternetLab, 2022.

Avenida Ipiranga 344 cj 11B | 01046-010 | São Paulo | SP | Brasil
ASSOCIAÇÃO INTERNETLAB DE PESQUISA EM DIREITO E TECNOLOGIA
www.internetlab.org.br

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Abreu, Jacqueline de Souza
O direito das investigações digitais no Brasil : fundamentos e marcos normativos / Jacqueline de Souza Abreu, Dennys Antonialli ; pesquisa e atualização do conteúdo Nathelie Fragoso, Eduarda Costa, Bárbara Simão ; supervisão Bárbara Simão, Francisco Brito Cruz ; colaboraram Heloisa Massaro e Laura Aliende da Matta. -- 3. ed. -- São Paulo : InternetLab, 2022.

Bibliografia.
ISBN 978-65-88385-14-2

1. Direito processual penal - Brasil **2.** Direitos fundamentais **3**. Processo penal **4.** Proteção de dados -Direitos - Brasil **5.** Proteção de dados - Leis e legislação **6.** Tecnologia e direito **7.** Tecnolgoias da informação e comunicação I. Antonialli, Dennys. **II.** Fragoso, Nathalie. **III.** Costa, Eduarda.**IV.** Duarte, Guilherme. **V.** Cruz, Francisco Brito. **VI.** Massaro, Heloisa. **VII.** Matta, Laura Aliende da.

22-12989 **CDU-343.1:004(81)**

Índices para catálogo sistemático:
1. Brasil : Direito e tecnologia : Direito processual penal **343.1:004(81)**
Aline Graziele Benitez - Bibliotecária - CRB-1/3129

< 1ª EDIÇÃO >

VIGILÂNCIA DAS COMUNICAÇÕES PELO ESTADO BRASILEIRO E A PROTEÇÃO A DIREITOS FUNDAMENTAIS (2015)

AUTORES: Jacqueline de Souza Abreu e Dennys Antonialli

< 2ª EDIÇÃO >

VIGILÂNCIA SOBRE AS COMUNICAÇÕES NO BRASIL (2017)

AUTORES: Jacqueline de Souza Abreu e Dennys Antonialli

< 3ª EDIÇÃO >

O DIREITO DAS INVESTIGAÇÕES DIGITAIS NO BRASIL (2022)

PESQUISA E ATUALIZAÇÃO DO CONTEÚDO: Nathalie Fragoso, Eduarda Costa, Bárbara Simão e Guilherme Duarte

SUPERVISÃO: Bárbara Simão e Francisco Brito Cruz

COLABORARAM: Heloisa Massaro e Laura Aliende da Matta

PROJETO GRÁFICO: Estúdio Claraboia

AGRADECIMENTO: VMCA Advogados

SUMÁRIO /

< 06 > APRESENTAÇÃO

< 08 > 1. PANORAMA NORMATIVO

< 10 > QUADRO 1: Princípios e direitos quanto ao sigilo das comunicações e à proteção de dados

< 12 > QUADRO 2: Marco Institucional

< 15 > QUADRO 3: Prerrogativas quanto ao acesso e guarda de dados

< 18 > QUADRO 4: Cooperação Jurídica Internacional em matéria penal

< 19 > 2. ANÁLISE: VIRTUDES E PROBLEMAS

< 20 > 2.1 Fragilidades de nível constitucional na proteção contra vigilância indevida

< 35 > 2.2 ANATEL: obrigações de guarda de dados nos serviços de telefonia

< 37 > 2.3 Receita Federal: obrigações fiscais de guarda de dados

< 39 > 2.4 Capacidades de acesso a dados com e sem contrapesos: telefonia vs. internet

< 56 > 2.5 Extraterritorialidade da legislação brasileira de proteção de dados pessoais

< 66 > 2.6 Interceptações: contrapondo teoria e prática

< 72 > 2.7 Infiltrações de agentes e coleta de dados

< 76 > 2.8 Acesso a dados sem transparência para fins de inteligência e segurança nacional

< 79 > 3. RECOMENDAÇÕES E BOAS PRÁTICAS NA PERSPECTIVA INTERNACIONAL

< 82 > 4. CONSIDERAÇÕES FINAIS

< 89 > NOTAS

APRESENTAÇÃO /

O objetivo deste livro, agora em sua terceira edição, permanece sendo o de oferecer um panorama sobre o quadro normativo que incide sobre as capacidades e prerrogativas de investigação sobre comunicações por autoridades estatais no Brasil. Além dos direitos e garantias previstos na Constituição Federal e dos dispositivos previstos na legislação, analisamos casos, notícias e decisões judiciais que tematizam as principais questões e representam as atuais controvérsias relacionadas a práticas de investigação sobre comunicações por autoridades no país. Para delimitar o escopo deste estudo, trabalhamos mapeando as atividades de investigações ou vigilância digital, ou seja, as que envolvem interceptações, monitoramento, análise, uso, guarda e obtenção de dados que incluam ou reflitam comunicações passadas, presentes ou futuras de alguma pessoa ou que surjam a partir delas.

Em 2015 e 2017, o InternetLab lançou estudos com objetivo e escopo semelhantes. Esta pesquisa constitui uma versão expandida e atualizada das anteriores.[1] Além de revisar o panorama normativo referente ao tema, o texto inclui sessões com temas novos, como por exemplo as discussões feitas sobre *(i)* novas divergências interpretativas sobre os direitos fundamentais ao sigilo das comunicações e à privacidade na Constituição Federal; *(ii)* os impactos da discussão sobre

proteção de dados em matéria penal; *(iii)* as referências legais aplicáveis a "infiltrações" de autoridades estatais, seja física ou virtualmente. O texto também inclui estatísticas sobre interceptações no país, agora atualizadas com dados de 2022.

Em linhas gerais, o leitor pode esperar deste livro a apresentação dos fundamentos e marcos normativos que envolvem investigações digitais no Brasil em 2022. Ele serve de guia para mapear a legislação aplicável ao tema no Brasil, seus pontos de conflito e divergência. Na seção final, podem ser encontradas recomendações elaboradas com base nos Princípios Internacionais sobre a Aplicação de Direitos Humanos na Vigilância das Comunicações.[2]

/ 1. PANORAMA NORMATIVO /

O quadro 1 apresenta um panorama geral sobre as normas constitucionais e legais gerais que impõem princípios e direitos quanto ao sigilo das comunicações e a proteção de dados no Brasil. O quadro 2 indica as instituições estatais associadas a práticas de investigação e vigilância, explicando suas funções. O quadro 3 resume a abrangência das prerrogativas estatais quanto ao acesso e guarda de dados sobre as comunicações, apresentando informações que serão detalhadas ao longo deste relatório. O quadro 4 aponta para a extensão que determinadas práticas de investigação envolvendo o Estado brasileiro podem assumir em decorrência de acordos e arranjos de cooperação judiciária internacional em matéria penal.

QUADRO 1.

PRINCÍPIOS E DIREITOS QUANTO AO SIGILO DAS COMUNICAÇÕES E À PROTEÇÃO DE DADOS NO BRASIL

DIREITOS	Constituição Federal garante o direito à liberdade de expressão, à intimidade, ao sigilo das comunicações e à proteção dos dados pessoais (art. 5º incisos IX, X, XII e LXXIX).
	Leis nº 9.472/97 (arts. 3º, V e IX, e 72) e nº 12.965/14 (art. 7º) garantem os direitos ao sigilo das comunicações e à privacidade no uso de telefonia e Internet.
	Lei nº 13.709/18 protege dados pessoais, a privacidade e a autodeterminação informativa, inclusive no que diz respeito a comunicações privadas.
	Não há testes consagrados, de aplicação uniformizada na jurisprudência e na doutrina, para avaliação da constitucionalidade de restrições a esses direitos.
	O art. 5º, § 2º da Constituição Federal dispõe que direitos e garantias nela expressos não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais de que o Brasil faça parte. Fazem parte do bloco de constitucionalidade, contudo, apenas tratados e convenções internacionais sobre direitos humanos aprovados em regime equivalente ao de emendas constitucionais, pelo art. 5º, § 3º.
REMÉDIOS	Em casos de violação a direitos, o cidadão pode impetrar habeas corpus ou mandado de segurança, previstos na Constituição (art. 5º, LXVIII e LXIX), ou propor ação ordinária.

GARANTIAS	Constituição Federal garante o devido processo legal, o contraditório e a ampla defesa, e a presunção de inocência (art. 5º, LIV, LV e LVII). Código de Processo Penal ordena que o juiz observe os princípios da adequação, da necessidade e da proporcionalidade ao ordenar produção de provas (art. 156). O mesmo vale para a apreciação de pedidos de medidas cautelares de produção de provas (art. 282). Intimação do atingido deve sempre ocorrer "ressalvados casos de urgência e de perigo de ineficácia" (art. 282, § 3º).
	Pela Constituição Federal (art. 5º, LVI) e pelo Código de Processo Penal (art. 157) são inadmissíveis provas obtidas por meios ilícitos, contrariando a Constituição ou a lei. I.e., não podem ser aproveitadas.
SANÇÕES	Art. 10 da Lei nº 9.296/96 criminaliza interceptações ilegais e quebra de segredo de justiça. Pena: reclusão de 2 a 4 anos e multa.
	Art. 154-A do Código Penal criminaliza invasão a dispositivo informático com o fim de obter dados. Pena: detenção de 3 meses a 1 ano, e multa. Se daí decorrer acesso a conteúdo de comunicação privada, a pena é reclusão de 6 meses a 2 anos, e multa.

QUADRO 2.

MARCO INSTITUCIONAL

ANATEL	Criada pela Lei nº 9.472/97, é órgão regulador responsável por organizar a exploração do setor de telecomunicações e fiscalizar a prestação de serviços a ele relacionados (art. 8º). Pode expedir resoluções (art.19). Para o exercício de suas funções e por meio das resoluções, cria obrigações de guarda de dados, de assistência em quebras de sigilo e interceptações, de identificação de usuários e de disposição de recursos para vigilância, e institui prerrogativas próprias de acesso a dados guardados.
RECEITA FEDERAL	Órgão do Ministério da Fazenda responsável pela administração de tributos internos e do comércio exterior, pela gestão e execução das atividades de arrecadação, fiscalização e investigação fiscal e pela atuação na cooperação internacional em matéria tributária e aduaneira (art. 15, Decreto nº 7.482/11). Tem acesso a documentos fiscais de empresas prestadoras de serviços de telecomunicações.
ANPD	A Autoridade Nacional de Proteção de Dados é uma autarquia de natureza especial responsável pela aplicação da Lei 13.709/2018, pela orientação e conformidade no tratamento de dados pessoais, realizado por agentes privados e autoridades públicas.

AUTORIDADES POLICIAIS

São órgãos de segurança. Pela Constituição Federal (art. 144), Polícias Civis estaduais e a Polícia Federal compõem a polícia judiciária. Pelo Código de Processo Penal, à polícia judiciária cabe a investigação de infrações penais e sua autoria (art. 4º), em procedimento com característica inquisitiva. O controle externo da sua atuação é exercido pelo Ministério Público (art. 129, VII, CF).

O Código de Processo Penal determina que, logo que tiver conhecimento de infração penal, a autoridade policial deverá colher todas as provas que servirem ao esclarecimento do fato (art. 6º, III). A Lei nº 12.830/13 prevê que, durante a investigação criminal, cabe ao delegado de polícia a requisição de perícia, informações, documentos e dados que interessem à apuração dos fatos (art. 2º, § 2º).

MINISTÉRIO PÚBLICO

Nos termos da Constituição Federal, o Ministério Público é órgão independente do Estado que serve à defesa da ordem jurídica, do regime democrático e de interesses indisponíveis (art. 127). São funções do Ministério Público promover ação civil pública, expedir notificações nos procedimentos administrativos de sua competência, requisitando informações e documentos para instruí-los e requisitar diligências investigatórias e a instauração de inquérito policial (art. 129).

A Lei Complementar nº 75/93 confere ao Ministério Público da União poder de requisitar informações e documentos a entidades privadas e realizar inspeções e diligências investigatórias no exercício de suas funções (art. 8º, IV e V), o que se aplica subsidiariamente aos MPs estaduais pelo art. 80 da Lei nº 8.625/93. Essa lei também prevê poderes de requisição de informações dos membros do Ministério Público (art. 26, III).

AUTORIDADES JUDICIAIS

Juízes podem ordenar de ofício produção de prova, nos termos do art. 130 do Código de Processo Civil e do art. 156 do Código de Processo Penal. Julgam requerimentos de autoridades policiais e do Ministério Público para produção de provas em investigações criminais e processo penal quando estas restringem direitos protegidos pela Constituição, como pedidos de quebra de sigilo.

CPIs

As Comissões Parlamentares de Inquérito, formadas temporariamente no seio do Poder Legislativo para apuração de fato determinado, são detentoras de "poderes de investigação próprios das autoridades judiciais" segundo o art. 58, § 3º da Constituição Federal. Podem ordenar quebra de sigilo de dados guardados e armazenados sem intervenção judicial.

ABIN E SISBIN

A Lei Complementar nº 75/93 confere ao Ministério Público da União poder de requisitar informações e documentos a entidades privadas e realizar inspeções e diligências investigatórias no exercício de suas funções (art. 8º, IV e V), o que se aplica subsidiariamente aos MPs estaduais pelo art. 80 da Lei nº 8.625/93. Essa lei também prevê poderes de requisição de informações dos membros do Ministério Público (art. 26, III).

ABIN não possui prerrogativas próprias para requisição de informações, mas pode obter dados na posse de órgãos que compõem o SISBIN, por previsão do Decreto nº 4.376/02 (art. 6-A e incisos). Segundo o decreto, a ABIN poderá requerer e manter representantes dos órgãos do SISBIN no Centro de Inteligência Nacional, que estarão dispensados das atribuições habituais no órgão de origem, mas poderão acessar respectivas bases de dados, "respeitadas as normas e limites de cada

instituição e as normas legais pertinentes à segurança, ao sigilo profissional e à salvaguarda de assuntos sigilosos." Além disso, desde a edição do Decreto 9.527/2018 a ABIN integra a Força-Tarefa de Inteligência, com competência para "analisar e compartilhar dados e de produzir relatórios de inteligência com vistas a subsidiar a elaboração de políticas públicas e a ação governamental no enfrentamento a organizações criminosas que afrontam o Estado brasileiro e as suas instituições".

QUADRO 3.

PRERROGATIVAS QUANTO AO ACESSO E GUARDA DE DADOS [PRÓXIMA PÁGINA]

FIM/ AUTORIDADE	REGULAÇÃO DAS TELECOMUNICAÇÕES (ANATEL)	INTELIGÊNCIA (SISBIN)
OBRIGAÇÕES DE GUARDA DE DADOS	Resoluções nº73/1998 e nº 738/2020 da ANATEL obrigam que dados relativos à prestação de serviço de telefonia fixa e móvel sejam guardados por prestadoras por, no mínimo, 5 anos e que dados relativos à conexão à Internet sejam guardados por provedores pelo prazo mínimo de 1 ano.	Não há obrigação de guarda expressamente para fins de inteligência.
ACESSO A DADOS ARMAZENADOS informações cadastrais e metadados	No exercício de poderes fiscalizatórios (art. 8º c.c. art. 19, Lei 9472/97), a ANATEL pode acessar documentos fiscais, que contêm informações cadastrais e registros, por requisição às prestadoras de serviço. Receita Federal também pode exigir acesso aos documentos fiscais (art. 11, Lei nº 8.218/91).	Poderes de requisição e de requerimento de dados da ABIN inexistentes. Possibilidade de acesso pelo SISBIN, nos termos dos arts. 6, V e 6-A do Decreto nº 4.376/02, por cooperação com outros órgãos.
ACESSO A COMUNICAÇÕES ARMAZENADAS conteúdo	Resoluções da ANATEL permitem acesso a gravações de ligações a serviços de atendimento ao cliente de prestadores de serviço de telecomunicações.	Poderes de requisição e de requerimento de dados da ABIN inexistentes. Possibilidade de acesso pelo SISBIN (arts. 6, V e 6-A do Decreto 4.376/02), por cooperação com outros órgãos.
ACESSO A COMUNICAÇÕES EM FLUXO interceptações	Prerrogativa de realização e competência de requerimento de interceptações inexistentes.	Prerrogativa de realização e competência de requerimento de interceptações da ABIN inexistentes. Lei 9.296/96 não estende tais poderes à ABIN. Há, contudo, possibilidade de cooperação entre órgãos pelo Sisbin para este fim (arts. 6, V e 6-A do Decreto 4.376/02).

LAW ENFORCEMENT (AUTORIDADES POLICIAIS, MINISTÉRIO PÚBLICO, JUÍZES E CPIs)

Lei nº 12.850/13 (art. 17) impõe a guarda de "registros de identificação dos números dos terminais de origem e de destino das ligações telefônicas" a empresas concessionárias de telefonia fixa e móvel, por 5 anos.

A Lei nº 12.965/14 (arts. 13 e 15) impõe a guarda de registros de conexão à Internet por 1 ano a todos os provedores de conexão e a guarda de registros de acesso a aplicações a provedores de aplicações com fins econômicos por 6 meses.

Pelas Leis nº 9.613/98 (art. 17-B) e nº 12.850/13 (art. 15), no caso de informações cadastrais de usuários de telefonia, o acesso pode ocorrer mediante simples requisição de autoridades policiais ou do Ministério Público às prestadoras. O acesso a registros telefônicos e outros metadados gerados no uso de telefonia (localização) não possui regulamentação legal específica: ocorre mediante ordem judicial para fins de produção de prova.
Os art. 13-A e 13-B do Código de Processo Penal autorizam o acesso a dados cadastrais sem ordem judicial e a "sinais" de localização, com autorização, em casos de crimes graves.
Pelo MS 23452/RJ do STF, acesso a registros telefônicos também pode ocorrer no âmbito de CPIs.

Pela Lei nº 12.965/14, acesso a informações cadastrais de assinantes de provedores de conexão e de usuários de aplicações de Internet pode ocorrer mediante requisição de autoridades competentes (art. 10, § 3º). No caso de registros de conexão à Internet e acesso a aplicações, acesso deve ocorrer por ordem judicial, quando houver fundados indícios de ocorrência de ilícito e utilidade dos registros à investigação ou instrução probatória, com necessidade de determinação de período específico (art. 22).

Lei 12.965/14 permite acesso a comunicações privadas registradas ocorridas por aplicações de Internet por ordem judicial (art. 7º, III). Código de Processo Penal autoriza buscas e apreensões mediante fundada suspeita de que alguém oculte consigo "objetos necessários à prova de infração ou à defesa do réu" e "cartas, abertas ou não, destinadas ao acusado ou em seu poder, quando haja suspeita de que o conhecimento do seu conteúdo possa ser útil à elucidação do fato" (art. 240, §2º). Segundo RE 418.416-8/SC, julgado pelo STF, mandado de busca e apreensão legitima acesso a dados armazenados em computadores.

Pela Lei 9.296/96, interceptações de comunicações telefônicas e de sistemas de informática e telemática podem ocorrer mediante ordem judicial, de ofício ou por requerimento de autoridade policial ou do Ministério Público, quando há indícios razoáveis de autoria ou participação em infração penal punida com pena de reclusão e indisponibilidade de outros meios de produção de prova (arts. 1º e 2º). Lei 12.965/14 permite interceptação de fluxo de comunicações via Internet na forma da Lei 9.296/96. Resoluções do CNJ e do CNMP especificam critérios a serem observados em pedidos e decisões.

QUADRO 4.

COOPERAÇÃO JURÍDICA INTERNACIONAL EM MATÉRIA PENAL

ACORDOS DE COOPERAÇÃO INTERNACIONAL EM MATÉRIA PENAL

O Brasil faz parte de vários acordos internacionais de assistência judicial recíproca que possuem implicações em termos de vigilância das comunicações, por permitirem auxílio na obtenção e produção de provas. Pelo princípio da dupla incriminação, a cooperação só pode ocorrer quando o ilícito sobre o qual se refere o pedido seja tipificado em ambos os países.

Exigem dupla incriminação	Acordos bilaterais com China, Coréia do Sul, Cuba, França e Portugal
Exigem dupla incriminação com exceções	Acordos bilaterais com Colômbia, Estados Unidos, Itália, México, Nigéria, Panamá, Peru, Reino Unido, Suíça, Suriname e Ucrânia e Acordos multilaterais no âmbito do Mercosul e da Organização dos Estados Americanos
Não exigem dupla incriminação	Acordos bilaterais com Espanha e Canadá

/ 2. ANÁLISE: VIRTUDES E PROBLEMAS /

2.1. FRAGILIDADES DE NÍVEL CONSTITUCIONAL NA PROTEÇÃO CONTRA VIGILÂNCIA INDEVIDA

A Constituição Federal contém, no rol dos direitos fundamentais, ao menos quatro incisos relevantes em matéria de limites à vigilância do Estado brasileiro sobre as comunicações. O inciso IV do art. 5º protege a dimensão positiva das comunicações, porquanto garante a liberdade de expressão ("IV - é livre a manifestação do pensamento, sendo vedado o anonimato"). Os incisos X e XII do mesmo artigo, por sua vez, protegem a liberdade negativa sobre as comunicações, ou seja, a faculdade de mantê-las em sigilo ou de, ao menos, limitar seus destinatários, ao preceituarem o direito à privacidade ("X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação") e o sigilo das comunicações ("XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal"). Finalmente, a Constituição passou a garantir o direito à proteção dos dados pessoais, inclusive nos meios digitais, com a aprovação da Emenda à Constituição nº 115, de 2022 que acrescentou o inciso LXXIX no artigo 5º da Constituição ("LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais"). Apesar de a Constituição proteger o sigilo das comunicações, a privacidade, e os dados pessoais disputas interpretativas ainda repercutem no grau de proteção que esses direitos garantem contra a vigilância indevida de autoridades do Estado sobre comunicações.

QUE SIGILO PROTEGEMOS?

A primeira fragilidade na proteção contra vigilância indevida do Estado decorre de uma persistente controvérsia sobre o âmbito de proteção conferido ao sigilo das comunicações, garantido no inciso XII do art. 5º ("XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal"). Da redação pouco clara do dispositivo, surgem basicamente duas questões interpretativas principais:

< I > qual é o objeto de proteção do sigilo: o *conteúdo* das informações comunicadas e transmitidas pelos meios citados (isto é, as correspondências, mensagens telegráficas, dados e telefonemas em si) ou o mero *fluxo* dessas informações por esses meios?

< II > qual(-is) grupo(-s), dentre os quatro listados no inciso, estão submetidos à exceção constitucional que permite a quebra do sigilo ("salvo, no último caso...")?

O entendimento doutrinário predominante[3], que também encontra eco em decisão do Supremo Tribunal Federal[4], é no sentido de que *(i)* a proteção do inciso XII do art. 5º não se refere ao conteúdo das informações comunicadas em correspondências, mensagens telegráficas, dados e telefonemas em si, mas sim à sua comunicação, isto é, ao seu *fluxo* enquanto ocorrem e que *(ii)* apenas o sigilo da comunicação por *telefonia*, enquanto está em fluxo, poderia ser restringido para fins de investigação criminal e instrução processual penal, não se estendendo essa possibilidade para o fluxo de dados, telegrafias e cartas.

Esse entendimento exclui do âmbito de proteção do dispositivo não somente o *conteúdo* de comunicações armazenadas, registradas ou gravadas, como também as informações geradas a respeito das circunstâncias nas quais as comunicações ocorreram (metadados). Em razão dessa limitação, diversos autores têm argumentado em favor de novas interpretações desse dispositivo, no sentido de levar em conta os avanços da tecnologia e as enormes quantidades de conteúdos e registros de comunicações que passaram a ser armazenadas em dispositivos pessoais, como computadores e aparelhos celulares. Diante disso, as disputas interpretativas a respeito da extensão dessa garantia constitucional reacenderam, tal como exploraremos abaixo.

Vale ressaltar que as questões interpretativas elencadas, surgidas assim que a Constituição Federal entrou em vigor, parecem bastante orientadas a identificar um núcleo *absoluto* de proteção do art. 5º, inciso XII, isto é, o núcleo essencial *inviolável*, cuja intromissão seria considerada sempre inconstitucional: por exemplo, pelo entendimento predominante apresentado acima, comunicações por correspondências, telegrafias e dados, enquanto em fluxo, seriam absolutamente invioláveis; somente comunicações telefônicas *em fluxo* poderiam ter seu sigilo afastado. Tal interpretação, mesmo que ainda respaldada por parte da doutrina, não reflete a jurisprudência dos tribunais, que passou a admitir "quebras" do sigilo do fluxo das comunicações de todos os tipos, isto é, não só de comunicações telefônicas, desde que "proporcionais", quando se fundamentarem em direito fundamental conflitante ou em interesse público. Também não reflete a atuação do Congresso Nacional que, em 1996, ao regulamentar a quebra de sigilo de comunicações telefônicas, como autoriza a Constituição Federal expressamente, também incluiu a possibilidade de se realizar interceptações "telemáticas" (o que abarca interceptações de "dados"). Em 2014, o Congresso

também voltou a explicitamente admitir interceptações de comunicações eletrônicas (que, igualmente, envolvem "dados") no Marco Civil da Internet.

NOVOS CAPÍTULOS CONSTITUCIONAIS SOBRE A PROTEÇÃO DE DADOS ARMAZENADOS

ADI 5527

Em seu voto na ADI 5527, que questiona a constitucionalidade dos artigos 10, parágrafo 2º, e 12, incisos III e IV do Marco Civil da Internet, empregados como fundamento de decisões judiciais que determinaram a suspensão do serviço do WhatsApp, a Ministra Rosa Weber exarou voto segundo o qual a disponibilização do conteúdo de comunicações privadas – em fluxo ou armazenadas – somente poderia ser determinada em ordem judicial, nas hipóteses e na forma que a lei estabelecer, para fins de investigação criminal ou instrução processual penal. Isso porque, apesar de reiterar a leitura de que o art. 5º, XII, da CF protegeria a comunicação dos dados, e o art. 5º, X, o sigilo de dados armazenados, a relatora destaca as limitações colocadas pelo art. 10, § 2º, da Lei nº 12.965/2014 às hipóteses de fornecimento de dados. Segundo ela, o dispositivo permitiria a disponibilização do conteúdo de comunicações privadas mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, seguindo a redação do art. 5º, XII da CF e transitando, portanto, no seu campo semântico.

O julgamento da ADI 5527 (e da ADPF 403, relatada pelo Ministro Edson Fachin) foi suspenso pelo pedido de vista do ministro Alexandre de Moraes, após o voto dos relatores das ações constitucionais examinadas em conjunto.

HABEAS CORPUS 168.052

Ao examinar o HC 168052, a 2ª Turma do Supremo Tribunal Federal reconheceu uma mutação constitucional para determinar que o acesso a aparelho celular por policiais sem prévia autorização judicial violava o sigilo das comunicações e da proteção de dados. A doutrina segundo a qual a inviolabilidade das comunicações não se aplicava aos dados armazenados conforme uma interpretação estrita da norma contida no art. 5º, XII, da CF/88, foi enfrentada e concluiu-se que, diante da Lei 12.965/2014 e das significativas alterações no contexto fático subjacente, seria preciso revisitar o âmbito de proteção dos direitos estabelecidos no art. 5º, X e XII, da CF e suas implicações.

No caso, foi declarada a ilicitude das provas ilícitas e derivadas decorrentes do acesso a aparelho celular por policiais sem autorização judicial, para verificação de conversas em aplicativo WhatsApp, e considerara superada a jurisprudência firmada no HC 91.867/PA.[5]

Finalmente, o relator pondera ainda pertinência de formalidades, entre as quais uma fórmula de garantia dos direitos das pessoas investigadas, como o aviso de Miranda, cuja inobservância leve à nulidade dos atos de investigação, que permitam o posterior controle da atuação mediante transcrição, assinatura e registro formal do depoimento dos investigados, com a declaração de ciência de seus direitos constitucionais.

GRADAÇÕES DE PRIVACIDADE: INFORMAÇÕES CADASTRAIS < METADADOS < CONTEÚDO?

Ainda que se considere que apenas o *fluxo* das comunicações seja objeto de proteção do sigilo previsto no inciso XII do art. 5º, a proteção à intimidade e à vida privada prevista pelo inciso X do mesmo artigo pode servir como fundamento para a proteção da privacidade de comunicações. A jurisprudência

e a doutrina admitem que esse inciso permite a proteção das comunicações de maneira mais ampla,[6] isto é, não só do seu fluxo, mas também do seu *conteúdo* e das informações sobre as circunstâncias em que ocorreram e entre quem se deram (o que pode ser revelado por informações cadastrais e metadados).

INFORMAÇÕES CADASTRAIS

Para fins deste estudo, consideram-se informações cadastrais todas aquelas que constarem do cadastro do cidadão junto a entidades dos setores público e privado, como, por exemplo, nome, filiação, endereço, número de telefone, e-mail, estado civil, profissão, tipo de serviço contratado, data de nascimento, dados pessoais como RG e CPF, entre muitos outros.

METADADOS

Para fins deste estudo, consideram-se metadados todos os dados e registros gerados incidentalmente a 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.

CONTEÚDO DAS COMUNICAÇÕES

Para fins deste estudo, considera-se conteúdo das comunicações todas as informações que dizem respeito à substância da comunicação, como, por exemplo, (o conteúdo de) uma conversa por telefone, o texto de um email ou de uma mensagem eletrônica ou o conteúdo de páginas da web.

Como se verá ao longo deste livro, a legislação infraconstitucional e a jurisprudência dos tribunais conferem diferentes níveis de proteção a essas diferentes categorias de informações, quais sejam, as **informações cadastrais**, os **metadados** e **conteúdo das comunicações** em si. Isso significa dizer que, dependendo do tipo de informação a que se quer ter acesso, o grau de proteção da privacidade sobre elas varia, como se umas fossem mais sensíveis que outras.

Para informações cadastrais, por exemplo, o entendimento que predomina é o de que são de menor relevância à privacidade. Em concreto, o que se vê são alterações legislativas que têm facilitado a obtenção dessas informações por requisição de autoridades, retirando a necessidade de ordem judicial.[7] Para quebra de sigilo de metadados, cujo tratamento legislativo varia conforme se refiram ao uso de telefonia ou de Internet, em geral se considera que basta ordem judicial fundamentada. Já para a realização de interceptações, ou seja, para que se tenha acesso ao conteúdo das comunicações enquanto em fluxo, por outro lado, entende-se que os fins estabelecidos pela Constituição e os requisitos específicos da lei regulamentadora devem ser respeitados, devendo ser o cumprimento deles controlado pela necessidade de ordem judicial.

Ao se adotar o entendimento de que o inciso XII, art. 5º, protege apenas o fluxo das comunicações, e se assumir que informações cadastrais e metadados são menos relevantes à privacidade, deixando-se de notar que a identificação final de usuários de serviços de telecomunicações é feita por cadastros e que informações de elevada relevância pessoal sobre personalidade, contatos e movimentação podem ser extraídas de metadados, os limites à vigilância do Estado brasileiro por meio de direitos fundamentais ficam fragilizados.

NOVAS QUESTÕES, VELHOS PROBLEMAS

Embora novas questões em torno da proteção do sigilo das comunicações e da privacidade venham surgindo, elas, em geral, retomam as mesmas controvérsias apontadas acima: o âmbito de proteção do sigilo das comunicações (art. 5, inciso XII), sua relação complementar com o direito à privacidade (art. 5, inciso X), e a diferenciação entre conteúdo, metadados e informações cadastrais. Podemos dividir essas novas roupagens de velhas disputas em três principais questões, discutidas abaixo.

(I) ACESSO A DADOS ARMAZENADOS EM DISPOSITIVOS ELETRÔNICOS MEDIANTE MANDADOS DE BUSCA E APREENSÃO

A interpretação constitucional restritiva dada ao sigilo das comunicações, qual seja a de que ele só protegeria (conteúdo de) comunicações enquanto estão em *fluxo*, gera uma situação de descompasso normativo: os modernos celulares, *tablets* e computadores armazenam uma enorme quantidade de informações, fotos e comunicações que oferecem retratos fiéis e detalhados de seus donos, mas que não gozariam da mesma proteção de comunicações em fluxo pelo mero fato de agora estarem arquivadas.

A Lei das Interceptações (Lei nº 9.296), de 1996, surgiu para regular a hipótese de aplicação da exceção constitucional ao sigilo das comunicações, determinando as circunstâncias nas quais as autoridades do Estado podem ter acesso a comunicações telefônicas e telemáticas enquanto estejam *em fluxo*, seja por meio da realização de interceptações junto a empresas de telefonia ou do emprego de grampos ou escutas ambientais. Para tanto, estabeleceu um regime jurídico rigoroso, que envolve o preenchimento de requisitos mais difíceis de serem atendidos em razão da grandeza da intrusão que a realização de interceptações junto a empresas de telefonia ou o emprego de grampos ou escutas ambientais acarretam. Esses requisitos

estão previstos no art. 2º da lei e exigem *(i)* a configuração de indícios razoáveis da autoria ou participação em infração penal; *(ii)* a inexistência de outros meios de prova; e *(iii)* o envolvimento em crimes de maior gravidade. A lei estabeleceu também um limite temporal para realização dessa medida (15 dias, renováveis).

Diferente é a situação da proteção (a conteúdo) de comunicações armazenadas, isto é, as que não estão mais em trânsito. A legislação infraconstitucional toca a questão em duas leis diferentes. Quando o acesso a essas comunicações se dá por meio de um intermediário, que detém os dados (como é o caso de provedores de aplicações de Internet), os dispositivos aplicáveis são aqueles previstos no Marco Civil da Internet, o qual determina que o acesso ocorra mediante "ordem judicial" (art. 7º, III) nas hipóteses e na forma que a lei o estabelecer (art. 10, § 2º), sem, entretanto, explicitar requisitos substantivos de padrão probatório. Quando o acesso se dá diretamente no aparelho apreendido, aplicam-se os dispositivos relativos à busca e apreensão, previstos no Código de Processo Penal (arts. 240 a 250). De acordo com os referidos dispositivos, fica autorizada a busca domiciliar e/ou pessoal quando há "fundada suspeita de que alguém oculte consigo" "objetos necessários à prova de infração ou à defesa do réu" e "cartas, abertas ou não, destinadas ao acusado ou em seu poder, quando haja suspeita de que o conhecimento do seu conteúdo possa ser útil à elucidação do fato" (art. 240, §2º).

Diante disso, pode-se dizer que, atualmente, comunicações armazenadas, registradas em celulares e computadores, provavelmente por anos a fim, gozam de um grau de proteção menor do que comunicações em *fluxo*, cujo acesso se encontra regulamentado de forma mais rigorosa pela Lei de Interceptações. Este paradoxo já começa a ser identificado e contestado em artigos de opinião.[8] Na doutrina,[9] também já se argumenta

que o art. 5º, XII da Constituição deveria garantir proteção irrestrita a *conteúdo* de comunicações, estejam elas em fluxo ou armazenadas, com a implicação de que toda quebra de sigilo de conteúdo deveria seguir os requisitos atuais da Lei das Interceptações, que regulamentou a exceção prevista constitucionalmente naquele inciso.

O Superior Tribunal de Justiça, em julgamento de outubro de 2021, afastou essa tese. No acórdão, a Quinta Turma determinou que dados constantes de aparelho celular obtidos por órgão investigativo são meios de prova lícita no processo penal quando há precedente mandado de busca e apreensão suficientemente fundamentado e expedido por juiz competente.[10] [11] No Recurso Extraordinário 418.416-8/SC, julgado em 2006, o Supremo Tribunal Federal também admitiu que o mero mandado de busca e apreensão já legitima acesso a dados armazenados em computadores. Apesar de separadas por quinze anos, as duas decisões demonstram quão penetrantes são as raízes do entendimento de que dados armazenados não estão protegidos pelo direito ao sigilo das comunicações na jurisprudência nacional, o qual alimenta o descompasso normativo entre a proteção de comunicações em fluxo e comunicações armazenadas.

Ainda não houve apreciação pelo plenário do STF sobre o argumento de que, no âmbito do acesso a dados no curso de um processo penal, todas as informações pessoais devem ser objetos de proteção, em observância à tese de que nenhum dado é irrelevante e todos podem ser utilizadas pelo Estado e por agentes privados de forma a prejudicar o titular. A questão deve ser apreciada pelo pleno no julgamento do Tema com Repercussão Geral 977, com o seguinte enunciado: "aferição da licitude da prova produzida durante o inquérito policial relativa ao acesso, sem autorização judicial, a registros e informações contidos em aparelho de telefone celular, relacionados à conduta delitiva e hábeis a identificar o agente do crime."[12]

(II) ACESSO A DADOS ARMAZENADOS EM DISPOSITIVOS ELETRÔNICOS APÓS PRISÃO EM FLAGRANTE

Quando autoridades policiais realizam prisões em flagrante, procedem à busca de objetos e produtos do crime portados pelo preso, para coleta de elementos que constituirão o auto de prisão em flagrante e como medida de segurança das próprias autoridades e encaminhamento para o distrito policial. Nesse cenário, tem-se questionado se é permitido às autoridades policiais acessar também dados armazenados no celular portado pelo preso. A prisão em flagrante autoriza a devassa não só à pessoa em si e/ou ao seu domicílio, mas também a tudo que está salvo eletronicamente junto em dispositivos do preso? Outra vez a controvérsia sobre o regime de proteção de dados (conteúdo de comunicações e metadados) *armazenados* surge.

Não há convergência nos tribunais superiores acerca da legalidade desse acesso e das provas daí obtidas. Em julgado de 2012, cujo posicionamento foi revisto pelo relator em caso recente[13], o STF decidiu que a análise de registros telefônicos (metadados) de celular apreendido após prisão em flagrante não caracteriza violação ao sigilo das comunicações (art. 5, inciso XII), porque sua proteção abarcaria "comunicações de dados e não dados em si" e porque "comunicação telefônica e registros telefônicos recebem proteção jurídica distinta".[14] Em 2007, o STJ já havia decidido de forma semelhante: a verificação de histórico de chamadas efetuadas e recebidas após prisão em flagrante não configura quebra ilegal de sigilo, porque as informações não foram obtidas por intermediário (empresas telefônicas) e nem se obteve conhecimento de conteúdo de conversas efetuadas.[15] Em 2017, por outro lado, agora lidando com um *smartphone* e demonstrando-se ciente da enorme quantidade de dados que um celular moderno produz e armazena, as duas turmas da Seção de Direito Penal do STJ tinham entendimento de ser ilícita a prova obtida diretamen-

te dos dados constantes de aparelho celular, decorrentes de mensagens de textos SMS, conversas por meio de programa ou aplicativos, como o WhatsApp, mensagens enviadas ou recebidas por meio de correio eletrônico, obtidos diretamente pela polícia no momento do flagrante, sem prévia autorização judicial para análise dos dados armazenados no telefone móvel.[16]

Por outro lado, em decisão de 2020, o STJ manteve o reconhecimento das peculiaridades do acesso às agendas telefônicas. Para a quinta turma do STJ, o art. 5º, inciso XII, da CF vedaria apenas o acesso a dados decorrentes de interceptação telefônica ou telemática, ainda que armazenados no aparelho celular, quando não houvesse autorização judicial. Dessa forma, o CPP autorizaria a apreensão do celular e o acesso aos dados constantes da agenda telefônica, que não estaria abarcada sob a garantia de proteção do sigilo telefônico ou dos dados telemáticos.[17] [18] No HC 168052, já abordado, a Segunda Turma do STF revê posicionamento anterior e decide que o acesso a dados contidos em aparelhos celulares é condicionado à prévia decisão judicial, afastando incidentalmente a distinção entre acesso a registros e conteúdo.

Cabe aqui menção à pesquisa lançada em 2019 pelo InternetLab sobre o retrato da jurisprudência dos tribunais estaduais no que tange o acesso de autoridades policiais a celulares em abordagens e flagrantes. Nela, conclui-se que a jurisprudência, apesar do precedente do STFM, não é uniforme na declaração da nulidade da prova decorrente do acesso ao celular da pessoa abordada por policiais e presa em flagrante sem ordem judicial. Em 86,5% dos acórdãos da justiça estadual analisados pela pesquisa, a prova obtida pelo acesso ao celular do acusado após a prisão em flagrante foi considerada lícita. O principal fundamento legal para estas decisões foi o art. 6º do Código de Processo Penal que autoriza a autoridade policial a apreender os objetos que tiverem relação com o fato típico

flagrante e colher as provas que servirem ao esclarecimento do fato e suas circunstâncias, inclusive o celular do acusado.[19]

Sobre a orientação da jurisprudência, cabem um esclarecimento e uma observação. A prisão em flagrante (art. 302 do Código de Processo Penal) só é justificada mediante certeza visual do crime e atualidade.[20] Isso significa que a situação de flagrante delito deve se configurar visualmente *antes* da prisão. Assim, enquanto está certo que a polícia deve proceder à apreensão de produtos e objetos do crime após prisão em flagrante, está bem menos certo que a prisão autorizaria não só a mera apreensão do aparelho celular, mas também a *busca* por informações nele contidas. A interpretação mais protetiva de direitos individuais argumentaria que a busca "virtual" deve depender de mandado específico[21], já que elementos prévios à apreensão do dispositivo já devem ser suficientes para a prisão. Do outro lado, a interpretação mais atenta às necessidades práticas de apuração de atividades criminosas desaconselharia tal necessidade[22], pois diminuiria a eficiência da atuação policial. Em todo caso, cabe demarcar a divergência teórica e jurisprudencial aqui, já que a admissão de buscas virtuais sem mandados pode representar uma expansão dos poderes de vigilância do Estado.

(III) UTILIZAÇÃO DE CRIPTOGRAFIA DE PONTA-A-PONTA: SEGURANÇA DAS COMUNICAÇÕES E IMPOSSIBILIDADE TÉCNICA DE INTERCEPTAÇÕES TELEMÁTICAS

Principalmente após a implementação da criptografia de ponta-a-ponta pelo WhatsApp, aplicativo de mensagens eletrônicas mais popular no país, em abril de 2016, o uso dessa tecnologia de proteção da confidencialidade de mensagens também se tornou motivo de controvérsia no Brasil. Isso, porque a implementação da criptografia de ponta-a-ponta inviabiliza a realização de interceptações telemáticas – a captura

das conversas de alvos específicos em tempo real, mesmo mediante ordem judicial. Como a empresa também não armazena mensagens pretéritas em seus servidores, não é possível obter o conteúdo de conversas no âmbito de investigações. Tal obstáculo técnico foi o pano de fundo das decisões de bloqueio contra o aplicativo.[23] Para os juízes envolvidos nesses casos, uma tecnologia que impede a realização de interceptações seria contrária à exceção prevista no inciso XII do art. 5º da Constituição Federal, que autorizaria o acesso a comunicações telefônicas em tempo real para fins de investigação criminal ou instrução processual penal. A questão motivou, inclusive, a abertura de inquérito civil pelo Ministério Público Federal em Rondonópolis/MT[24] bem como sinalizações, na opinião pública[25] [26], sobre a necessidade de regular o uso dessa tecnologia.

Entre 2015 e 2016, as três decisões judiciais ordenaram a suspensão das atividades do WhatsApp, sob o fundamento de que a empresa responsável pelo aplicativo se negava a disponibilizar à autoridade judiciária o conteúdo de mensagens privadas trocadas por usuários submetidos a investigação criminal. Nesse sentido, a empresa argumentou que utiliza um sistema de criptografia ponta-a-ponta, de forma a tornar tecnicamente inviável o acesso a dados e consequente cumprimento das decisões judiciais. O WhatsApp destacou que essa ferramenta desempenha função de proteger os direitos constitucionais de liberdade de expressão, comunicação, e privacidade, delimitados tanto na CF quanto no MCI.

O STF, na ADPF 403 e na ADI 5527, que analisam a compatibilidade de bloqueios do WhatsApp com a Constituição Federal, também foi instado a se manifestar sobre a o impasse. Na sessão do dia 28.05.2020, os ministros relatores das ações, a Ministra Rosa Weber e o Ministro Edson Fachin, proferiram seus votos. O objeto da ação é a possibilidade de suspensão do WhatsApp por determinações judiciais, conforme a leitura

empregada nas referidas decisões dos artigos 10, §2º, e 12, III, do Marco Civil da Internet.[27]

Mais uma vez, o que se discute é o alcance da proteção constitucional ao sigilo das comunicações. Em se tratando de tecnologia imprescindível para a confidencialidade de dados, a discussão envolve também necessariamente privacidade, liberdade de expressão, proteção de dados e segurança individual, coletiva e nacional.

Diante da tensão entre os direitos postos, os relatores iniciaram o julgamento dessa ADI e APDF destacando que o sigilo das comunicações, inclusive pela internet, é uma garantia constitucional. Em seus votos, os relatores afastam qualquer interpretação do MCI que permita que as empresas deem acesso ao conteúdo de mensagens criptografadas ponta-a-ponta, mesmo que por meio de ordem judicial. Para os relatores, é inviável qualquer determinação judicial que possa enfraquecer a proteção criptográfica de aplicações da internet. Ainda, segundo os ministros, a lei obriga as empresas à guarda apenas de metadados, referentes ao usuário e à utilização do aparelho.[28] Porém, o julgamento foi suspenso e não há previsão para que o STF se posicione sobre a constitucionalidade do MCI e a extensão da criptografia para não acesso aos dados pessoais.

Apesar da amplitude constitucional da questão, vale também destacar que, atualmente, não há na legislação brasileira obrigação oponível aos desenvolvedores de aplicativos de mensagens no sentido de construírem interceptações. É importante destacar que a interceptação difere da quebra de criptografia, esta permite acesso a todo conteúdo antes criptografado, ou seja, só as pessoas que conhecem a chave da criptografia conseguem entender a mensagem passada enquanto aquela é medida judicial por tempo limitado para acesso ao fluxo de comunicações em sistemas de informática e telemá-

tica e é regulada pela Lei nº 9.296, de 24 de julho de 1996. Isso, porque as obrigações previstas na Lei das Interceptações e em resoluções da ANATEL se destinam apenas a empresas de telefonia e provedores de conexão, mas não a provedores de aplicações de Internet.[29]

CRIPTOGRAFIA NO PROJETO DE LEI GERAL DE PROTEÇÃO DE DADOS NO ÂMBITO PENAL

No fim de 2019, a Câmara dos Deputados instituiu comissão de juristas responsável por propor o anteprojeto para a "LGPD penal". A comissão foi presidida pelo ministro do Superior Tribunal de Justiça, Nefi Cordeiro, e composta por outros 13 membros. Ao fim de aproximadamente um ano de trabalho, apresentou um anteprojeto inspirado, principalmente, na própria LGPD e na Diretiva 680/2016 da União Europeia.

O anteprojeto define como lícita a adoção de criptografia ponta-a-ponta e exime o destinatário de ordem da obrigação diante da incapacidade técnica resultante do emprego de mecanismo de proteção de dados que torne impossível o cumprimento da ordem judicial (arts. 11, §3º c.c. 59, § 2º). O anteprojeto, no entanto, ainda não foi formalmente apresentado no Congresso Nacional.

2.2. ANATEL: OBRIGAÇÕES DE GUARDA DE DADOS NOS SERVIÇOS DE TELEFONIA

No exercício de sua competência normativa (art. 19 da Lei nº 9.472/97), que exerce através da edição de *resoluções*, e no exercício de sua função de regulação das telecomunicações, a Agência Nacional de Telecomunicações (ANATEL) organiza a prestação de serviços e concretiza direitos de usuários, mas

não sem criar significativo potencial de vigilância. A falta de precisão e clareza de suas resoluções e de transparência em sua atuação colaboram para a fragilidade da proteção de usuários de serviços de telecomunicações à vigilância do Estado. As principais regulações que incitam a vigilância permanecem pouco alteradas ao longo dos anos, de forma a perpetuar as práticas de vigilância da agência.

OBRIGAÇÕES DE PRESTADORES DE SERVIÇOS DE TELECOMUNICAÇÕES

A Resolução nº 738/2020, que alterou as Resoluções 426/05 e Resolução nº 477/07 – substituindo-as no que diz respeito ao sigilo, prevenção à fraude e ações de apoio à segurança pública –, obriga, no Art. 65-J., que sejam mantidos "os dados relativos à prestação de serviços, incluindo, conforme o caso", sejam guardados os documentos de natureza fiscal, dados cadastrais dos assinantes e dados de bilhetagem e das ligações efetuadas e recebidas, bem como data, horário, duração e valor da chamada pelo prazo mínimo de 5 (cinco) anos, nos serviços de telefonia, e registros de conexão à Internet pelo prazo mínimo de 1 (um) ano. Não há normas específicas de segurança sobre a forma como devem ser guardados os dados: o art. 65-H apenas estabelece que é responsabilidade das prestadoras zelar pelo sigilo das comunicações e pela confidencialidade dos dados. No art. 65-K, determina-se que as prestadoras tornem disponíveis os recursos tecnológicos, dados e facilidades necessárias à suspensão de sigilo das telecomunicações, decorrente e nos limites de ordem judicial. Por meio desta resolução, são, portanto, estabelecidas obrigações de retenção em massa de dados e de assistência técnica para quebra de sigilo de comunicações.

Essa alteração não significou uma alteração substancial à vigilância autorizada pela agência.[30]

A lógica da obrigação de guarda de dados relativos à prestação de serviço de telefonia por 5 anos estabelece obrigações de guarda de dados na telefonia fixa e móvel. Com base nisso, sustentou-se, por longo período, a conveniência da disposição desses dados para fins investigatórios e persecutórios do Estado. A Lei nº 12.850/13 ("Lei das Organizações Criminosas"), que obrigou empresas de telefonia a guardarem dados expressamente para estes fins, é apenas de 2013. Além disso, os termos da resolução instituem obrigações de guarda de dados mesmo quando os tipos de serviço se referem a tarifas fixas *(flat rates)*, quando a duração de uma chamada ou o número a que se ligou não afetam a cobrança final do usuário que será tributada. A extrapolação da vigilância da ANATEL para outros fins fica, portanto, evidenciada.[31]

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.

2.3. RECEITA FEDERAL: OBRIGAÇÕES FISCAIS DE GUARDA DE DADOS

O art. 65-J da Resolução nº 738/20 da ANATEL, visto acima, revelou que a lógica da obrigação de guarda de dados cadastrais e registros telefônicos por 5 anos está intimamente ligada às obrigações fiscais e ao art. 11 da Lei nº 8.218/91, o qual obriga pessoas jurídicas a manterem documentos fiscais à disposição da Receita Federal pelo prazo decadencial previsto na

legislação tributária. Isso significa que não só a ANATEL, mas a própria Receita Federal, no exercício de suas funções de administração e fiscalização fiscal, pode ganhar acesso a informações sobre comunicações de usuários, através da solicitação de documentos fiscais que contenham esses dados (no caso da telefonia móvel e fixa, ao menos os registros de chamadas, hora, data, duração e valor da chamada, associados a informações cadastrais).

Como a obrigação de manter "documentos fiscais" à disposição da Receita Federal se estende à toda pessoa jurídica, a prerrogativa da Receita Federal tem potencial de atingir todo usuário de serviços de telecomunicações no Brasil, sempre que tais documentos fiscais forem capazes de revelar informações sobre o comportamento comunicativo do usuário, mesmo que apenas a partir de metadados e informações cadastrais.

A Oficina Antivigilância identificou, em julho de 2015, a celebração de acordo entre o Departamento de Segurança Nacional dos Estados Unidos, pela Agência de Fiscalização de Aduana e Proteção de Fronteiras, e o Ministério da Fazenda do Brasil, por meio da Secretaria da Receita Federal, para "reconhecimento mútuo" dos Programas de "Parceria Aduana-Empresa contra o Terrorismo" da agência americana e de "Operador Econômico Autorizado" da Receita Federal, o que envolveria transferência de infraestrutura de processamento de dados e desenvolvimento e uso de tecnologia da informação em comum.[32] Considerando que a Receita Federal tem acesso a informações sobre comunicações de brasileiros, essa cooperação pode significar ampliação da vigilância a nível internacional.

2.4. CAPACIDADES DE ACESSO A DADOS SEM E COM CONTRAPESOS: TELEFONIA VS. INTERNET

Leis federais recentes normatizaram capacidades de acesso a dados no exercício de atividades de segurança pública *(law enforcement)*: a edição da Lei das Organizações Criminosas, a promulgação do Marco Civil da Internet, do Pacote Anticrime, que alterou o Código de Processo Penal, e da Lei Geral de Proteção de Dados são exemplos relevantes.

LEI DAS ORGANIZAÇÕES CRIMINOSAS (LEI Nº 12.850/13)

OBRIGAÇÃO DE GUARDA DE REGISTROS TELEFÔNICOS

A Lei das Organizações Criminosas, determina, em seu art. 17, que "as concessionárias de telefonia fixa ou móvel manterão, pelo prazo de 5 (cinco) anos, à disposição das autoridades mencionadas no art. 15 [delegado de polícia e Ministério Público], registros de identificação dos números dos terminais de origem e de destino das ligações telefônicas internacionais, interurbanas e locais". Se, de um lado, a temática da lei em que foi inserida tal obrigação – Lei das Organizações Criminosas – sugere o fim legítimo a que tal obrigação pretende servir, qual seja, garantir a eficácia de investigações criminais e do processo penal, de outro, revela a impertinência da inserção nessa lei: o acesso a dados guardados com base no art. 17 não se restringe aos cidadãos suspeitos, acusados ou processados pelos crimes praticados por organização criminosa. A inserção de uma obrigação geral, abrangente, em uma lei específica pode ter camuflado o aumento de capacidades do Estado que ela representa, já que isso passou praticamente despercebido no debate público e acadêmico, não tendo sido objeto de escrutínio em termos de legalidade, necessidade e proporcionalidade, nem acompanhada de

especificações sobre dados a serem registrados, destinatários, limites e condições de uso e medidas de segurança. A constitucionalidade deste dispositivo foi contestada na ADI 5063/DF, que está conclusos para julgamento desde 2020 e da qual se falará mais a seguir.

PRERROGATIVAS DE ACESSO A DADOS CADASTRAIS

O art. 15 da Lei das Organizações Criminosas dispõe ainda que "o delegado de polícia e o Ministério Público terão acesso, independentemente de autorização judicial, apenas aos dados cadastrais do investigado que informem exclusivamente a qualificação pessoal, a filiação e o endereço mantidos pela Justiça Eleitoral, *empresas telefônicas*, instituições financeiras, *provedores de internet* e administradoras de cartão de crédito" (grifo adicionado). Tal disposição repete o art. 17-B da Lei dos Crimes de Lavagem de Dinheiro (Lei nº 9.613/99), incluído pela Lei nº 12.683/2012.

Tais normas, que previram a desnecessidade de ordem judicial para o acesso a tais informações, são fruto de recentes reformas legislativas. Anteriormente, a possibilidade de quebra de sigilo de dados cadastrais sem autorização judicial era motivo de controvérsia na doutrina e na jurisprudência. Isso porque, apesar de o art. 6º do Código de Processo Penal, no inciso III, permitir à autoridade policial "colher todas as provas que servirem para o esclarecimento do fato e das circunstâncias" quando tiver notícia da prática de infração penal[33], e a Lei Complementar nº 75/93, em seu art. 8º, inciso IV, permitir ao Ministério Público da União a requisição de "informações e documentos a entidades privadas" no exercício de suas atribuições, o que se aplica subsidiariamente aos organismos estaduais (art. 80 da Lei nº 8.625/93), o acesso a tais informações era rejeitado pelas empresas com base no argumento de que estariam protegidas pela proteção constitucional da

privacidade do art. 5º, inciso X, da Constituição Federal, sendo necessária ordem judicial para quebra do sigilo.[34]

Nesse contexto, os recentes dispositivos atendem a pressões das autoridades investigativas para ter o "acesso direto" – por mera requisição – expressamente legislado, o qual contribuiria para a eficácia, em termos de rapidez, de investigações e processos. Mesmo antes da sanção de tal previsão legal, autoridades policiais já defendiam a interpretação segundo a qual dados cadastrais não seriam resguardados pelos dispositivos constitucionais que protegem a privacidade e o sigilo das comunicações (art. 5, incisos X e XII), porque não se confundiriam com conteúdo de comunicações telefônicas. Em 2016, acolhendo tal posicionamento, o Tribunal Regional Federal da 3ª Região sustentou que a operadora Claro, que em 2013 impetrou mandado de segurança contra ofícios da Polícia Federal requisitando dados cadastrais de chips apreendidos, tem a obrigação de revelar os dados de cadastro mesmo sem ordem judicial.[35]

Cabe ainda ressaltar que, apesar de a possibilidade de acesso a tais informações por mera requisição às empresas estar prevista nas leis sobre crimes de organização criminosa e de lavagem de dinheiro, as autoridades citadas pretendem também que o acesso por requisição não esteja limitado apenas a investigações e persecuções no âmbito de tais crimes, uma vez que o legislador não teria expressamente limitado tais competências apenas aos fins das leis em que se inserem.[36] Na prática, tais autoridades utilizam essas previsões para fundamentarem requisições de dados a prestadoras de serviços de telefonia; apenas se a companhia negar o pedido é que a questão é analisada judicialmente.

PRERROGATIVA DE ACESSO TAMBÉM A REGISTROS TELEFÔNICOS?

Desde a promulgação da Lei das Organizações Criminosas, as autoridades competentes, mas principalmente delegados de polícia, também têm requisitado registros telefônicos a companhias telefônicas *sem* autorização judicial, com base em interpretação combinada dos arts. 15, 17 e 21 desta Lei. Pelo já citado art. 15, "o delegado de polícia e o Ministério Público terão acesso, independentemente de autorização judicial, apenas aos dados cadastrais do investigado que informem exclusivamente a qualificação pessoal, a filiação e o endereço" mantidos por empresas telefônicas e provedores de internet. O art. 17 obriga, entretanto, as companhias à guarda de "registros de identificação dos números dos terminais de origem e de destino das ligações telefônicas internacionais, interurbanas e locais" por 5 anos, os quais serão mantidos "à disposição das autoridades mencionadas no art. 15". O *caput* do art. 21, por sua vez, criminaliza a recusa ou omissão de "dados cadastrais, registros, documentos e informações requisitadas pelo juiz, Ministério Público ou delegado de polícia, no curso de investigação ou do processo", com pena de reclusão de 6 meses a 2 anos, e multa. Diante disso, tais autoridades têm requisitado, além dos dados cadastrais, registros telefônicos (e alguns até dados de localização), sem autorização judicial. Requisições diretas são feitas a empresas, sob ameaça de que serão punidas, caso não colaborem. Ação Direta de Inconstitucionalidade (ADI 5063/DF, acima citada) foi proposta perante o Supremo Tribunal Federal contra tais artigos pela Associação Nacional de Operadoras Celulares (ACEL), sob fundamento de violação ao direito à privacidade e ao princípio da legalidade, dada a insegurança jurídica acarretada pela imprecisão das normas.[37] A ação, proposta originalmente em 2013, ainda está pendente de julgamento, como descrito anteriormente.

OBRIGAÇÕES DE GUARDA DE DADOS

No que se refere aos registros de conexão, preceitua o art. 13 do Marco Civil da Internet que "na provisão de conexão à Internet, cabe ao administrador de sistema autônomo [como Embratel, Oi, UOL Diveo e muitos outros como universidades públicas, por exemplo] respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento". Destinatários da obrigação, os "administradores de sistema autônomo" são, segundo o art. 5º, IV da lei, "a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País", atingindo assim todo provedor de acesso à Internet que preencha tal definição.[38] Objeto da guarda, os registros de conexão, são, segundo o art. 5º, inciso VI, "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". O art. 14, em atenção aos riscos à privacidade de usuários da rede, proíbe que provedores de conexão guardem registros de acesso a aplicações.

O art. 15 do Marco Civil da Internet determina, por sua vez, que "o provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento". Aplicações, segundo inciso VII do art. 5º, são o

"conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet". O destinatário da obrigação aqui não é todo provedor de aplicação, mas apenas aqueles que exerçam tal atividade empresarialmente. Provedores não comerciais de aplicações, podem, contudo, mediante ordem judicial, ser obrigados a guardar dados, "desde que se trate de registros relativos a fatos específicos em tempo determinado", conforme determina o § 1º do art. 15. Os dados abrangidos pela obrigação geral de registro são, de acordo com a definição do art. 5º, inciso VIII, "o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP".

No que concerne à obrigação de guarda de registros de conexão à Internet e acesso a aplicações em geral, são pertinentes ainda quatro comentários. Primeiro, o § 2º do art. 13 e o § 2º do art. 15 admitem requisição cautelar de extensão do tempo de guarda dos dados, não havendo previsão, entretanto, de prazo máximo dessa extensão. Segundo o art. 10, § 4º, além dos próprios *caputs* dos arts. 13 e 15, referem-se a medidas de segurança para a guarda e disponibilização dos registros, e o art. 12, a sanções por violação dessas normas. Terceiro, o decreto nº 8.771/2016, que regulamentou o Marco Civil da Internet, estabelece diretrizes sobre formato de armazenamento e padrões de segurança na guarda de dados e registros e determina que dados retidos devem ser excluídos tão logo atingida a finalidade de seu uso ou o prazo determinado em lei (arts. 13 a 16). Quarto, alguns julgados em tribunais estaduais têm determinado, apesar das delimitações expressas do Marco Civil da Internet vistas aqui quanto a "registros", a guarda e exibição de informações relativas à "porta lógica de origem" utilizada por usuários, por parte de provedores de conexão[39] e de aplicação de internet.[40] [41]

VEDAÇÃO AO ANONIMATO E DEBATE SOBRE PORTA LÓGICA NO BRASIL

O Marco Civil criou obrigações de retenção de dados para possibilitar a identificação dos usuários na internet e a responsabilização por atos ilícitos. O artigo 13 obriga os provedores de conexão à manutenção dos registros de conexão pelo prazo de 1 ano. No artigo 15, determina ao provedor de aplicações a manutenção dos registros de acesso a aplicações de internet pelo prazo de 6 meses. Registros de conexão 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 dados" (art. 5, VI do MCI), e os registros de acesso 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 (art. 5, VII do MCI).

No contexto de transição decorrente do esgotamento dos endereços de IPV4, no entanto, os endereços de IP podem não ser suficientes à identificação de um usuário. Isso porque entre as ferramentas para contornar temporariamente este esgotamento está o "compartilhamento" de um IP entre computadores, utilizando uma etiqueta para a identificação do usuário de um IP compartilhado, a porta lógica. O MCI, no entanto, não prevê a guarda de portas lógicas.

Essa questão vem sendo enfrentada pelos Tribunais, levados à decidir entre uma interpretação literal ou extensiva de um dever de retenção geral, que afeta provedores de internet e usuários da rede.[42] [43]

PRERROGATIVAS DE ACESSO A DADOS CADASTRAIS

O Marco Civil da Internet dispõe, no § 3º do seu art. 10, que o respeito à proteção a dados pessoais e comunicações privadas garantido no *caput* do artigo "não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e ende-

reço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição". Acerca de tal previsão, membros da comunidade acadêmica e da sociedade civil solicitavam que o decreto regulamentador do Marco Civil da Internet esclarecesse os limites desse acesso, delimitando expressamente as autoridades competentes.[44] Com relação a essa demanda, o decreto nº 8.771/16, que regulamentou o Marco Civil da Internet, limitou-se a elencar informações que podem ser categorizadas como "dados cadastrais" (filiação, endereço e qualificação pessoal entendida como nome, prenome, estado civil e profissão) – sem obrigar que sejam colhidas – e a determinar que, no ato de requisição, a autoridade administrativa indicará o "fundamento legal de competência expressa para o acesso e a motivação para o pedido de acesso aos dados cadastrais" (art. 11). O decreto também institui a obrigação de órgãos da administração federal de publicar anualmente estatísticas sobre pedidos (art. 12). O decreto não se manifestou acerca de requisições de informação cadastral feitas a partir de dado de registro de acesso à aplicação (endereço de IP e horário), que, em princípio, poderiam burlar a necessidade de ordem judicial que abranja a quebra do sigilo de registro de conexão à Internet.[45]

ACESSO A REGISTROS DE CONEXÃO À INTERNET E DE ACESSO A APLICAÇÕES

O art. 10, § 3º, do Marco Civil da Internet prevê explicitamente que a disponibilização dos registros de conexão à Internet e de acesso a aplicações só poderá ser feita por ordem judicial, proteção repetida nos arts. 13, § 5º e 15, § 3º. O art. 22, por sua vez, delimita os fins a que isso poderá ocorrer, qual seja a formação de "conjunto probatório em processo judicial cível ou penal", e estabelece os requisitos a que deve atender o requerimento da "parte interessada" para a concessão da ordem judicial: funda-

dos indícios da ocorrência do ilícito; justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e período ao qual se referem os registros. O art. 23, por fim, encarrega ao juiz a responsabilidade de "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".

Em atenção à utilidade do acesso a registros de aplicações na internet e dos mecanismos legais de quebra de sigilo de várias pessoas e não apenas daqueles interessados no processo penal, o STF vai decidir se é constitucional a decretação judicial da quebra de sigilo de dados telemáticos de um conjunto não identificado de pessoas em procedimentos penais. Esse tema teve a repercussão geral reconhecida no meio de 2021 com o Recurso Extraordinário (RE) 1301250, no Tema 1.148. No caso, está em questão a decisão judicial do Tribunal do Rio de Janeiro (RJ) que determinou a quebra de sigilo de um grupo indeterminado de pessoas que fizeram pesquisas relacionadas à ex-vereadora do RJ Marielle Franco e a sua agenda nos quatro dias anteriores ao atentado em que ela e seu motorista foram assassinados, em 2018. As empresas Google Brasil Internet Ltda. e Google Inc. questionam as ordens que buscam, através do fornecimento de registros de acesso, dados de dispositivo e dados cadastrais, os usuários que pesquisaram, em um período de cinco dias, certas palavras-chave que constituem critérios alternativos de busca.

A ministra relatora do recurso, Rosa Weber, considera fundamental a fixação de uma tese sobre questão constitucional inserida neste caso. Para a ministra, o debate sobre a compatibilização entre a proteção de dados pessoais e a quebra de sigilo toca garantias constitucionais fundamentais que devem ser apreciadas e que possuem alto potencial de repetitividade no

cenário jurisdicional brasileiro. O Ministério Público Federal defende que é permitido o afastamento de sigilo de dados telemáticos, no âmbito de procedimentos penais, ainda que em relação a pessoas indeterminadas, condicionado a parâmetros de fundamentação específica, delimitação de tempo do acesso e garantia de sigilo no compartilhamento da informação. O processo está dependente de julgamento.

A QUEBRA DE SIGILO E AS LIMITAÇÕES DAS ORDENS JUDICIAS

A jurisprudência tem se reiterado há aproximadamente trinta anos na remissão ao parecer escrito em 1992 pelo jurista Tércio Sampaio Ferraz Júnior, intitulado "Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado". O texto tem sido uma das principais matrizes para interpretação do artigo 5º, X e XII, e para a definição do conteúdo do direito ao sigilo das comunicações. Segundo a interpretação dos julgadores, a inviolabilidade do sigilo de dados protegeria apenas o fluxo de dados, não se aplicando aos dados armazenados.

Embora tenha revisitado o texto mais de uma vez, apontando a distância entre a questão factual abordada em 1993 e o atual contexto de desenvolvimento tecnológico, o jurista retomou a questão no parecer juntado ao RE n.º 1301250 representativo do Tema 1148, sobre os casos de quebra de sigilo proferidas no inquérito policial que investiga o assasinato da vereadora Marielle. O jurista afirma que 'não se pode negar que dados armazenados e estáticos podem constituir informações e atividades das mais sensíveis à privacidade de indivíduos".

"A interpretação do art. 5º, XII não pode excluir a necessidade de se analisar o impacto de medidas investigativas estatais sob o próprio prisma da intimidade e da vida privada (art. 5º,

x) e do mais recentemente reconhecido direito à proteção de dados pessoais. Isto é: ainda que uma medida não interfira na relação intersubjetiva atinente à comunicação de dados, isso não significa que não há violação a direito à privacidade ou à autodeterminação informativa em questão. Pelo contrário, pode existir – também através de dados em si estáticos – os mais graves assaltos à integridade moral de indivíduos". Segundo Ferraz Júnior, estaríamos em um cenário de mutação constitucional, em que a proteção de dados não se esgota apenas na vida privada e a confidencialidade deve ser buscada pelos agentes sociais, para que a internet não seja apenas ambiente para buscas generalizadas e exploratórias de possíveis suspeitos em investigação.[46]

A "RASTREABILIDADE" DE DADOS EM DISCUSSÃO NO PL Nº 2.630/20

O Projeto de Lei nº 2.630/20, do senador Alessandro Vieira (Cidadania-SE), busca instituir a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet (conhecido como "PL das *fake news*"). Buscando criar medidas de combate à disseminação de conteúdo falso nas redes sociais e serviços de mensagens privadas, o projeto trazia disposições sobre a retenção de dados por aplicativos de comunicação. Segundo a proposta, estes aplicativos passariam a ser obrigados a reter, por três meses, "registros dos envios de mensagens veiculadas em encaminhamentos em massa".

A medida foi amplamente debatida pelo potencial de violar direitos fundamentais à privacidade e à proteção de dados. O dispositivo impunha a obrigatoriedade de retenção preventiva de registros de data e horário das mensagens, além do número de destinatários que as recebessem. Dentre as críticas, coloca-

-se o fato de que criaria uma infraestrutura de monitoramento necessariamente vinculada ao conteúdo das mensagens, o que poderia levar ao fim da criptografia de ponta a ponta e a efeitos inibidores à liberdade de expressão. Criticou-se, também, a proporcionalidade e eficácia da medida em evitar disseminação de conteúdos ilícitos.

Em substitutivo ao projeto apresentado pelo deputado Orlando Silva, a regra ganhou novos contornos. Na nova versão, afirma-se que "a autoridade judicial pode determinar aos provedores de serviço de mensageria instantânea a preservação e disponibilização dos registros de interações de usuários determinados por um prazo de até 15 (quinze) dias, [...], vedados os pedidos genéricos ou fora do âmbito e dos limites técnicos do seu serviço". Veda-se, além disso, a associação desses registros ao conteúdo das comunicações.[47]

ACESSO A COMUNICAÇÕES PRIVADAS ARMAZENADAS

Como se mencionou anteriormente, a quebra de sigilo de conteúdo de comunicações eletrônicas em posse de provedores de aplicações de Internet (tais como Google e Facebook) está também prevista no Marco Civil da Internet, nos arts. 7º, III e 10, § 2º, os quais explicitam a necessidade de ordem judicial para tanto. Ao contrário do que ocorre para o fornecimento de registros (art. 22), entretanto, a lei não trata explicitamente dos requisitos formais e materiais que devem ser satisfeitos para que a ordem judicial seja concedida,[48] o que dá margem a abusos e aplicações casuísticas.

Para limitar esse tipo de acesso a casos em que é legítimo e apropriado, é possível interpretar o silêncio da lei à luz da Constituição Federal, do instituto análogo da busca e apreensão do Código de Processo Penal e de precedentes de tribunais superiores que lidaram com o tema, como o HC 315.220/RS do STJ.[49] Em se tratando de conteúdo de comunicações, o pedido

de quebra de sigilo deve apresentar fundados indícios de ocorrência de ilícito penal e indícios de autoria e/ou participação contra o alvo investigado. Em atenção ao princípio da proporcionalidade, deve ser provado que a medida é adequada à instrução, sendo pertinente para o crime investigado com base em fatos já configurados. Quanto à necessidade, essa fonte de prova deve ser imprescindível ao prosseguimento da investigação e consecução do arcabouço probatório, bem como delinear o período ou abrangência dos dados a serem coletados em íntima correlação aos elementos concretos do caso investigado.[50] A ordem judicial concedida deve ser minuciosamente fundamentada também nestes termos, em atenção ao art. 93, IX da Constituição Federal.

CASOS RELEVANTES

QUEBRAS DE SIGILO NA FALTA DE REGULAÇÃO PARA A TELEFONIA

A vigilância da telefonia para fins de garantia da segurança pública *(law enforcement)* é improvisada na Lei das Organizações Criminosas. Não há lei sistematizadora que regulamente obrigação de guarda, hipóteses em que o acesso pode ser efetuado, nem os fins a que pode servir. Isto é, não há um tipo de "Marco Civil da Telefonia", que limite capacidades de investigação. Não há restrições a que a quebra de sigilo só ocorra no âmbito criminal, excluindo o uso em casos cíveis, ou que se limite a registros de chamadas (ligações recebidas e efetuadas, data, hora e duração), sobre os quais há as obrigações de guarda vistas anteriormente, e não atinja dados de localização (Estações Rádio Base, por exemplo). Isso leva à consequência prática de que o sigilo sobre *quaisquer* metadados gerados em telefonia é quebrado *sempre* que ordem judicial o determinar. Sintomático disso é o caso julgado pelo Tribunal de Justiça do Rio Grande do Sul em julho de 2007, que admitiu a possibilidade de quebra de

sigilo de dados de localização de usuário de celular devedor de alimentos, nos autos de execução dessa obrigação. O réu em tal ação foi condenado ao pagamento de pensão alimentícia; não realizando o pagamento, nem justificando a impossibilidade de fazê-lo, teve sua prisão decretada. Sua localização foi tentada repetidas vezes, sem sucesso. Em face disso, e em nome da "proteção integral a crianças e adolescentes", a desembargadora admitiu que uma "interceptação telefônica", como a chamou, fosse efetuada com o fim de levantar dados sobre a localização do devedor a partir de seu número de celular.[51]

MARCO CIVIL E LIMITAÇÕES DE ACESSO A DADOS NA INTERNET

O Marco Civil da Internet, por outro lado, soma frutos em termos de limitação contra acessos indevidos a dados de comunicações. A Justiça Federal de São Paulo anulou, em decisão de abril de 2015,[52] requisição de delegado da Polícia Federal ao Twitter pelo "máximo de dados possíveis, como o IP de acesso da máquina do responsável, datas de acesso, qualificação completa dos responsáveis e dados cadastrais do usuário @EnkiEa666". A Polícia Federal alegou que o § 3º do artigo 10 do Marco Civil da Internet "prevê a possibilidade de requisição de dados cadastrais pelas autoridades administrativas e a Lei n. 12.830/2013 expressamente autoriza que os Delegados de Polícia, no curso do inquérito policial, requisitem dados e informações de interesse às investigações", em referência ao art. 2º, § 2º de tal lei. Em sua decisão, o juiz federal reconhece que a requisição feita pela autoridade policial abrange não apenas dados cadastrais de usuários, mas também registros de acesso a aplicação e afirma: "a lei [o Marco Civil] permite às autoridades administrativas, com competência para tanto, requisitar informações aos provedores de internet referentes aos seus usuários, desde que tais informações se limitem a dados cadastrais, como qualificação pessoal, filiação e endereço.

Entendo, pois, que informações relacionadas aos registros de conexão e de acesso a aplicações de internet, bem como de dados pessoais e do conteúdo de comunicações privadas, dependem de autorização judicial, como expressamente previsto no referido § 1º, do art. 10, da Lei nº 12.965/14". No que se refere aos dados cadastrais, o juiz acolhe esclarecimento do Twitter no sentido de que não possuiria informações como nome completo, endereço e filiação do usuário, e, quanto aos registros de acesso a aplicação, rejeita a obrigação de disponibilização dos dados, dada a ausência de ordem judicial que a ampare.

NOVOS PODERES DE ACESSO A DADOS NO CÓDIGO DE PROCESSO PENAL: AS LEIS Nº 13.964/19 E 13.344/16

Em dezembro de 2019, foi aprovada a Lei 13.964/19, o chamado Pacote Anticrime, que alterou o CPP e, entre outras mudanças, criou a figura do juiz das garantias, autoridade responsável pelo controle da legalidade da investigação criminal e pela garantia dos direitos individuais do acusado. Esse juiz passaria a ser competente para decidir sobre a interceptação telefônica, do fluxo de comunicações em sistemas de informática e telemática ou de outras formas de comunicação, e o afastamento dos sigilos fiscal, bancário, de dados e telefônico (art. 3º-B, CPP). Assim, as definições dos limites de atuação das atividades de persecução penal e sigilo das comunicações e dos dados seriam determinadas, no caso concreto, por esse juiz. Porém, a implementação do juiz das garantias está suspensa por decisão do Ministro Fux, em medida cautelar na ADI 6.298/DF.

Em outubro de 2016, foi aprovada a Lei nº 13.344, que dispõe sobre prevenção e repressão ao tráfico interno e internacional de pessoas e medidas de atenção às vítimas. Entre suas inovações, estão dois artigos adicionados ao Código de Processo Penal (CPP). O novo art. 13-A do CPP autoriza, para certos crimes

listados,[53] ao membro do Ministério Público ou delegado de polícia a "requisitar a quaisquer órgãos do poder público ou de empresas da iniciativa privada dados e informações cadastrais da vítima ou de suspeitos". Além disso, enunciando requisitos formais para requisição (indicação de nome da autoridade requisitante, unidade de polícia responsável e número do inquérito), estabelece o prazo de 24h para seu atendimento. Com isso, como ocorre também no âmbito da Lei das Organizações Criminosas e da Lei dos Crimes de Lavagem de Dinheiro, torna-se desnecessária a apresentação de ordem judicial para o acesso a dados cadastrais por parte dessas autoridades para a investigação dos referidos crimes previstos no dispositivo.

O novo art. 13-B, por sua vez, confere poderes de vigilância com o fim de localizar suspeitos e vítimas de tráfico de pessoas, determinando que "se necessário à prevenção e à repressão dos crimes relacionados ao tráfico de pessoas, o membro do Ministério Público ou o delegado de polícia poderão requisitar, mediante autorização judicial, às empresas prestadoras de serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso".

Nos detalhes, a redação do dispositivo apresenta ambiguidades, como por exemplo: *(i)* o *caput* do art. 13-B menciona "crimes relacionados a tráfico de pessoas", sem indicar expressamente a que tipos penais se refere; *(ii)* o mesmo artigo menciona também "meios técnicos" que permitam localizar pessoas: "sinais, informações e outros"; sem especificar quais seriam as "informações", muito menos o que se deve entender por "outros". De acordo com a definição genérica, vale tudo para localizar alguém – só não estaria diretamente incluída no pacote a quebra de sigilo de conteúdo de comunicações, que precisam de autorização específica (art. 13-B, § 2º, I). De acordo

com o § 2º do art. 13-B, o "sinal" deve ser fornecido por período não superior a 30 dias (inciso II), renovável por igual período. Em uma redação confusa, o inciso III do mesmo parágrafo afirma que "para prazos superiores (ao que trata o inciso II), será necessária ordem judicial", o que poderia sugerir que não seria necessária a ordem para prazo inferior. O § 4º também abre espaço para uma interpretação que dispensa a necessidade de autorização judicial: se não houver manifestação judicial em até 12h após o pedido, as "empresas de telecomunicação e/ou telemática" terão de fornecer os dados mesmo sem a autorização, "com imediata comunicação ao juiz".

Em janeiro de 2017, a Associação Nacional das Operadoras de Celular (ACEL) propôs ação direta de inconstitucionalidade (ADI 5642) contra esses dispositivos, por violarem os art. 5º, incisos X e XII da Constituição.[54] O julgamento desta ADI foi iniciado em 2021, oportunidade que o Ministro Relator Edson Fachin julgou improcedente o pedido de declarar inconstitucional o art. 13-A do CPP e dar interpretação conforme ao art. 13-B do CPP para inadmitir autorização genérica que obrigue as empresas prestadoras de serviço de telecomunicações e telemática a disponibilizarem os meios técnicos que permitam a localização da vítima ou dos suspeitos do delito em curso, nos crimes de tráfico de pessoas. O julgamento foi interrompido por pedido de vista do Ministro Nunes Marques.

A LEI GERAL DE PROTEÇÃO DE DADOS É TÃO GERAL ASSIM?

Aprovada em 2018, a Lei Geral de Proteção de Dados (LGPD) trata de maneira ampla e sistemática a proteção de dados pessoais no país. Por ser uma lei geral, a LGPD é aplicada de forma ampla ao tratamento, uso, coleta, armazenamento, de qualquer informação vinculada a pessoa física, porém, por previsão expressa, ela não incide sobre o tratamento de dados realizados para fins de segurança pública, defesa nacional, se-

gurança do Estado; ou atividades de investigação ou repressão de infrações penais (art. 4º, III, da LGPD).

Ao mesmo tempo que a lei estabelece essa exceção, ela determina que o tratamento de dados no âmbito criminal deve atender medidas de proporcionalidade, o devido processo legal, e o interesse público, além de observar os princípios de proteção de dados previstos na LGPD e os direitos dos titulares. Ainda, deverá ser editada uma lei específica sobre essa forma de tratamento de dados. Além disso, desde então, foi aprovada a Emenda Constitucional que previu expressamente o direito à proteção de dados pessoais no art. 5º, LXXIX, da Constituição Federal, obrigando, assim, todos os poderes do Estado em sua realização.

Portanto, o tema não ficou descoberto. As autoridades que tratam dados para os fins observados estão obrigadas a observar princípios e regras de proteção de dados pessoais na seara criminal, ainda que haja pouca clareza sobre o respectivo impacto neste campo da ação estatal.

2.5. A EXTRATERRITORIALIDADE DA LEGISLAÇÃO BRASILEIRA DE PROTEÇÃO DE DADOS PESSOAIS

O *caput* do art. 11 do Marco Civil da Internet determina que provedores de conexão e aplicações de Internet respeitem a "legislação brasileira e os direitos à privacidade, à proteção de dados pessoais e ao sigilo das comunicações privadas e dos registros" "em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações em que pelo menos um desses atos ocorra em território nacional". Nos parágrafos que seguem, a lei esclarece que a obrigação de respeitar a legislação brasileira no tratamento de dados se aplica

< I > aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil (art. 11, §1º); e

< II > 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 (art. 11, § 2º).

O escopo delineado no artigo atinge também empresas unicamente sediadas fora do país e, por isso, pode-se dizer que inaugura um regime de alcance extraterritorial da lei brasileira no que diz respeito a essas questões. Literalmente, o artigo institui o dever de que mesmo essas empresas estrangeiras respeitem a legislação nacional em atividades de tratamento de dados. Na prática, entretanto, ele tem sido utilizado para exigir que também observem a legislação material e processual brasileira relativa ao acesso de autoridades a dados de usuários.[55] De fato, estudos sobre o processo de elaboração do Marco Civil da Internet apontam que essa redação abrangente tentou justamente endereçar dificuldades práticas para obtenção de acesso a dados por parte de autoridades, porquanto, sob o argumento de que os dados estariam guardados no exterior, obedecendo, portanto, à legislação de outro país e só podendo ser obtidos por procedimento de assistência judiciária internacional específico, provedores não atendiam a ordens judiciais de quebra de sigilo.[56]

A inclusão desses dispositivos não estancou esse problema - e pode até tê-lo piorado. Uma das forças por trás dos bloqueios do aplicativo WhatsApp em todo o país, para além da criptografia, foi justamente a recusa da empresa em fornecer alguns dados a autoridades brasileiras fora dos mecanismos de cooperação internacional.[57] Assim, essa interpretação do

dispositivo (segundo a qual empresas estrangeiras devem entregar dados mediante direta apresentação de requisições e/ou ordens de autoridades brasileiras) pode aumentar significativamente os poderes de vigilância do Estado brasileiro. Mais promissora, em termos de proteção de garantias individuais contra uma vigilância *sem fronteiras* e de garantia da efetividade do processo, seria a dedicação a iniciativas que procuram modernizar processos de assistência mútua entre países (MLATS), hoje burocráticos e demorados e intrinsecamente pensados na territorialidade *física*.

Contudo, essa perspectiva, ainda que favorável e desejável, não é a que vêm sendo acolhida majoritariamente pela jurisprudência pátria: ao contrário, derroga-se a cooperação com organismos estrangeiros em prol de uma intensificação da prática do Estado brasileiro em exercer o poder coercitivo, seja ele por meio de multas pesadas ou por ameaças de bloqueio em caso de não cooperação.

ORIGENS DO PROBLEMA: OS INEFICIENTES ACORDOS DE COOPERAÇÃO MÚTUA E OS CONTORNOS CINZENTOS DE JURISDIÇÃO NA INTERNET – JACQUELINE DE SOUZA ABREU

Para entender as origens do impasse entre autoridades de investigação e empresas sediadas no exterior, para além dos termos legais do Marco Civil da Internet, é preciso ter em mente o conceito de "jurisdição", que, no direito internacional público, consiste basicamente na autoridade de exercer poder sobre pessoas e coisas em um determinado território.[58] Como um Estado detém jurisdição dentro de seus limites geográficos, tornou-se necessária a instrumentalização de meios de cooperação internacional para situações nas quais autoridades públicas de um

Estado-nação esbarram nos limites de seu poder, como quando precisam extraditar suspeitos, ouvir testemunhas ou colher provas que se encontram no exterior.[59] Para este fim, são tradicionalmente utilizadas cartas rogatórias e celebrados acordos de cooperação mútua entre países, por exemplo. Como indicado no Quadro 4, o Brasil faz parte de mais de 30 acordos bilaterais e multilaterais de assistência judicial recíproca em matéria penal.

Esse modelo funcionou com sucesso – e, na maior parte das situações, ainda funciona –por duas razões centrais. Primeiro, porque, em geral, é um esquema idealizado para situações raras e excepcionais. Na grande maioria dos processos, não há que se realizar extradições, ouvir testemunhas estrangeiras nem obter provas no exterior. Segundo, porque a identificação dos limites da jurisdição e da necessidade de se recorrer a meios de cooperação é relativamente simples para meios físicos: se autoridades do país A precisam de pessoas ou documentos fisicamente localizados no território do país B, o país A necessariamente precisa solicitar cooperação do país B, já que não pode exercer poder fora de seu território.

A questão assumiu contornos mais complexos com a Internet. Primeiro, porque a necessidade de colheita de *provas digitais* armazenadas em computadores no exterior ou detidas por empresas sediadas no exterior se tornou uma atividade cotidiana. Segundo, porque "documentos digitais" (dados em geral como informações cadastrais, registros, conteúdo de comunicações), ao mesmo tempo em que de fato estão localizados em servidores físicos em (ao menos um) lugar certo, também podem ser acessados virtualmente de diversos lugares do mundo. Além disso, as "pessoas" que detém o controle sobre os servidores onde os dados estão armazenados e/ou sobre o acesso a eles, os provedores de aplicações de Internet, estão presentes multinacionalmente, seja por sedes e subsidiárias ou apenas virtualmente.

Quando se recusam a fornecer dados de usuários mediante direta requisição e/ou ordem de autoridade brasileira, fora dos trâmites dos acordos de cooperação internacional, empresas de Internet se baseiam nessas doutrinas clássicas a partir das quais se edificaram os limites jurisdicionais e a construção de acordos de cooperação mútua – os fatos de que os dados buscados como evidência digital estão fisicamente armazenados no exterior e/ou detidos por pessoa estrangeira. Não há nada de desafiador à soberania nacional quando assim o fazem; pelo contrário, o modelo de cooperação internacional foi pensado para conciliar o respeito a diferentes nações.

Apesar disso, a emergência de leis *extraterritoriais* ou pelo menos de interpretações *extraterritoriais* do escopo de obrigações de cooperação com autoridades estatais na entrega de dados de usuários tem colocado provedoras transnacionais de serviços de internet em situações complicadas, quando as diferentes legislações nacionais a que estão simultaneamente submetidas estão em conflito, isto é, quando obedecer a uma implica desrespeitar outra. É frequentemente este o caso do embate do Brasil com empresas norte-americanas, já que a legislação americana aplicável ao fornecimento de dados de usuários a autoridades proíbe provedores de entregar *conteúdo* de comunicações sem a apresentação de um *warrant* emanado por um juiz americano.

Uma saída para remediar esta situação é reformular o atual modelo de cooperação judiciária internacional em matéria penal e repensar os fatores definidores de jurisdição sobre dados digitais como elementos de prova, atendendo às necessidades de autoridades de segurança pública ao redor do mundo e respeitando direitos humanos. Enquanto isso não ocorre, ameaças de multas, prisões, bloqueios, além de inúmeros acordos "informais"[60] entre empresas e autoridades serão frequentes.

A VIA MULTILATERAL: CONVENÇÃO DE BUDAPESTE

A Convenção de Budapeste, um tratado multilateral originalmente concebido na UE e ratificado por seus membros em 2001, busca promover a harmonização dos ordenamentos jurídicos das partes no âmbito penal material e processual penal no que tange aos crimes cometidos no âmbito digital. Em 2021, o Brasil tornou-se parte do acordo, tendo sido promulgada através do Decreto Legislativo 37/2021.

No âmbito material, a Convenção obriga os Estados à inclusão de tipos penais nas respectivas legislações para viabilizar a punição de crimes cometidos na internet (que vão desde a pirataria, até crimes de relacionados à exploração à produção, disseminação e posse de material sexualmente explícito que inclua crianças e adolescentes). Já no âmbito processual, a Convenção obriga as partes a legislar para prever meios de obtenção de prova para interceptação e acesso a dados armazenados. Além disso, pode ela própria constituir o fundamento jurídico para cooperação internacional em matéria penal entre os signatários, caso não exista tratado ou acordo entre as partes ou estas decidam aplicá-la em substituição ao tratado ou acordo existente.

A via multilateral acelera o esforço de integração em cooperação internacional, inserindo os países numa rede que facilita o intercâmbio de informações. É possível dizer, no entanto, que não soluciona de pronto os problemas hoje associado aos acordos bilaterais que podem substituir, caso as partes assim o decidam. O arcabouço normativo oferecido pela Convenção também carece de estrutura institucional, capaz de operacionalizá-lo. Além disso, questiona-se a aptidão do diploma, na ausência de salvaguardas específicas e órgãos de controle, para prevenir arbitrariedades e obstar a configuração de uma rede internacional de vigilância detrimental aos direitos fundamentais dos indivíduos.[61]

CASOS RELEVANTES: UMA LISTA COM GOOGLE, YAHOO, MICROSOFT E FACEBOOK

Os tribunais brasileiros tendem majoritariamente a afirmar a sua autoridade para determinar o fornecimento direto de dados de usuários a plataformas de Internet, isto é, sem necessidade de recorrer a procedimentos de cooperação internacional. Há inúmeros casos emblemáticos. Em 2013, no Inquérito nº 784/CF, a Google Brasil Internet Ltda. impetrou mandado de segurança contra ofício da Polícia Federal pelo qual se requisitou a quebra de sigilo telemático de contas do *Gmail*. A empresa alegou que *(i)* não tem acesso aos computadores que armazenam os dados; *(ii)* os computadores em que os dados estão armazenados estão nos Estados Unidos; *(iii)* os computadores são operados e os dados são detidos pela sua controladora, Google Inc., a qual está proibida de fornecer dados a autoridades estrangeiras fora da via diplomática (tratado bilateral de cooperação jurídica).

A ministra Laurita Vaz do Superior Tribunal de Justiça (STJ) rejeitou os argumentos apresentados pela Google Brasil, afirmando que "o fato de esses dados estarem armazenados em qualquer outra parte do mundo não os transforma em material de prova estrangeiro, a ensejar a necessidade da utilização de canais diplomáticos para transferência desses dados". Segundo observou, "o que se pretende é a entrega de mensagens remetidas e recebidas por brasileiros em território brasileiro, envolvendo supostos crimes submetidos induvidosamente à jurisdição brasileira". Também asseverou que "remeter o Poder Judiciário Brasileiro à via diplomática para obter dados é afrontar a soberania nacional, sujeitando o Poder Estatal à inaceitável tentativa da empresa em questão de se sobrepor às leis pátrias [...]". A Microsoft Informática Ltda. já desafiou ordens de quebra de sigilo de e-mails *Hotmail* em termos semelhantes à Google Brasil e o resultado de derrota no STJ foi o mesmo.[62]

Esporadicamente, alguns julgados, que não chegam a se constituir como uma posição ou sequer uma expectativa de revisão do entendimento majoritário, caminham no sentido de amparar a via da cooperação internacional, em detrimento das soluções de força bruta. A diferenciação entre subsidiária/encarregada de publicidade e matriz/operadora da plataforma ajudou, por exemplo, o Facebook. Em novembro de 2016, a Justiça Federal do Rio Grande do Sul decidiu que o Ministério Público Federal (MPF) deveria obter conteúdo de comunicações privadas transmitidas na rede social Facebook pela via diplomática, uma vez que tais dados são controlados pela Facebook Inc. e/ou Facebook Ireland Limited.[63] A subsidiária brasileira Facebook Serviços Online do Brasil Ltda., que usualmente recebe as ordens judiciais com determinações de fornecimento de dados, vêm argumentando reiteradamente em diversos processos que apenas presta serviços relacionados a publicidade, não detendo informações relativas a usuários, e que, sempre que recebe requerimentos de autoridades brasileiros, encaminha-os para os efetivos operadores da rede social. Nos autos de Ação Civil Pública proposta pelo MPF contra a Facebook Brasil contra os mesmos "reiterados descumprimentos de ordem judicial", a empresa também acumula vitórias na primeira e na segunda instância da Justiça Federal, que indeferiram a ação por razões formais: falta de interesse de agir e impossibilidade do pedido.[64] Em 2018, o STJ consagrou a vitória da rede social no julgamento dos embargos de declaração opostos pelo MPF contra as decisões que identificaram os vícios processuais da demanda.

Na prática, o que se verifica é que o judiciário brasileiro tende a cada vez mais fortalecer a posição segundo a qual as empresas de Internet atuantes no Brasil deverão se submeter às ordens judiciais brasileiras que demandem o fornecimento de informações, mesmo que o fornecimento contrarie o ordenamento jurídico dos países onde estão sediadas.

Desde 2017, quando foi publicada a versão anterior deste estudo, este quadro se agravou. Recentemente, a 5ª Turma do STJ, em duas ocasiões (em recurso da Facebook[65] e da Yahoo[66], fixou a tese de que a simples ordem judicial era suficiente para ensejar o acesso a dados hospedados no exterior, sem a necessidade de mecanismos de cooperação internacional pois "Por estar instituída e em atuação no País, a pessoa jurídica multinacional submete-se, necessariamente, às leis brasileiras, motivo pelo qual se afigura desnecessária a cooperação internacional para a obtenção dos dados requisitados pelo juízo".[67]

Frisa-se ainda que a solução encontrada para impor o cumprimento das ordens judiciais de acessos a dados das empresas com controladoras e bases sediadas fora do país vêm sendo a de impor pesadas multas e ameaças de restrição de funcionamento no país (como bloqueios). Vale, nesse sentido, destacar a Ação Declaratória de Constitucionalidade nº 51[68], que tramita no Supremo Tribunal Federal. Impetrada pela Associação de Empresas Brasileiras de Tecnologia da Informação ("Assespro") e com relatoria do Min. Gilmar Mendes, a ação busca a declaração da constitucionalidade do mecanismo de cooperação internacional entre Brasil e Estados Unidos da América (em inglês, MLAT - "Mutual Legal Assistance Treaty"), promulgado pelo Brasil através o Decreto 3.810/2001.

A ação ainda não foi julgada, mas a liminar foi parcialmente deferida em 13/05/2019 pelo relator Gilmar Mendes, proibindo a movimentação dos valores das sanções impostas nos casos em que se discute a aplicação do MLAT. Na prática, não houve pronunciamento sobre a impossibilidade de se aplicar multas, mas somente da impossibilidade de se destinar os valores.

RELATÓRIOS DE TRANSPARÊNCIA DE EMPRESAS DE INTERNET: PEDIDOS DE AUTORIDADES BRASILEIRAS

Muitas empresas de Internet divulgam semestralmente estatísticas sobre pedidos de dados que receberam de autoridades estatais. Abaixo reunimos as informações divulgadas por Google, Microsoft, Facebook e Twitter em seus relatórios de transparência já publicados que contiveram informações sobre pedidos advindos de autoridades brasileiras.[69] Tais estatísticas dizem respeito a todos os pedidos por dados que as empresas receberam (e não necessariamente que foram atendidos), sem discriminação do tipo de pedido entre informações cadastrais, metadados e conteúdo de comunicações.

PEDIDOS DE DADOS FEITOS POR AUTORIDADES BRASILEIRAS A EMPRESAS DE INTERNET

	GOOGLE	MICROSOFT	FACEBOOK	TWITTER
2010	4.239	–	–	–
2011	2.318	–	–	–
2012	2.777	–	–	39
2013	2.324	2.592	1.880	42
2014	1.468	2.461	2.519	127
2015	1.686	2.600	2.920	83
2016	1.884	2.471	3.570	96
2017	2.391	2.315	4.585	106
2018	3.759	2.043	7.261	100
2019	6.567	2.440	12.232	168
2020	10.648	2.570	18.617	332
2021	7.543 (1º SEM.)	2.955	26.648	267 (1º SEM.)

2.6. INTERCEPTAÇÕES: CONTRAPONDO TEORIA E PRÁTICA

A TEORIA: LEI DAS INTERCEPTAÇÕES TELEFÔNICAS E RESOLUÇÕES DO CNJ E DO CNMP

A Lei nº 9.296/96 ("Lei das Interceptações Telefônicas") disciplina esse procedimento. O parágrafo único do art. 1º desta Lei estende o âmbito de sua aplicação também a "interceptação do fluxo de comunicações em sistemas de informática e telemática", o que compreende, portanto, o fluxo da comunicação de dados pela Internet, como *emails*. No contexto da controvérsia em relação à correta interpretação a ser dada ao dispositivo constitucional que protege o sigilo das comunicações, a constitucionalidade de tal dispositivo foi contestada, com base no entendimento apresentado de que só o fluxo de comunicações *telefônicas* poderia ser restringido para fins de persecução penal.[70] Entretanto, em razão de vício formal, a ação direta de inconstitucionalidade proposta não foi julgada no mérito; nova ação de mesmo escopo (ADI 4.112/DF) ainda aguarda julgamento. Atualmente, o Marco Civil da Internet, em seu art. 7º, inciso II também prevê a possibilidade de interceptação do fluxo de comunicações pela Internet, mediante ordem judicial, "na forma da lei" (em referência à Lei de Interceptações).

A interceptação do fluxo das comunicações é feita, segundo o *caput* do art. 1º da Lei 9.296/96, para fins de prova em investigação criminal e em instrução processual penal, por autorização judicial, ordenada de ofício ou mediante requerimento de autoridade policial ou do Ministério Público (art. 3º). Em razão de tais previsões, fica proibida a realização de interceptações por autoridades não nomeadas, como a Agência Brasileira de Inteligência (ABIN). O art. 2º restringe ainda mais as hipóteses de seu uso: ela não é admitida quando *não* houver indícios razoáveis da autoria ou participação em in-

fração penal; quando a prova puder ser feita por outros meios disponíveis; quando o fato investigado constituir infração penal punida, no máximo, com pena de detenção (comum em crimes de menor gravidade). O parágrafo único do art. 2º e os arts. 4º e 5º garantem, por sua vez, que a interceptação só ocorrerá quando devidamente fundamentada: deve estar amparada em descrição clara da situação objeto da investigação, inclusive com a indicação e qualificação dos investigados, salvo impossibilidade manifesta, devidamente justificada; o pedido deve demonstrar sua necessidade para a apuração da infração e os meios a serem empregados; a decisão indicará a sua forma de execução. O art. 5º prevê que a interceptação não poderá exceder 15 dias, podendo ser estendida, contudo, por autorização judicial: é "renovável por igual tempo uma vez comprovada a indispensabilidade do meio de prova". Apesar de tal artigo permitir a interpretação de que o prazo máximo da medida é de 30 dias, jurisprudencialmente[71] prevaleceu o entendimento de que a medida pode ser estendida *enquanto* indispensável. Essa tese foi cristalizada em tese de repercussão geral pelo STF[72], isso é, uniformizou-se um entendimento válido para todos os outros casos submetidos ao julgamento da corte. Nessa ocasião, entendeu-se que as prorrogações sucessivas de interceptações telefônicas são lícitas desde que "fundamentada e demonstrada a necessidade da medida com a apresentação de elementos concretos e da complexidade da investigação".[73]

O art. 7º dá à autoridade policial o poder de requisitar "serviços e técnicos especializados às concessionárias de serviço público" para os procedimentos de interceptação. O art. 8º ordena o sigilo no tratamento das gravações e o art. 9º, a sua inutilização, quando não interessarem a fins de prova. Interceptações ilegais são criminalizadas no art. 10. Por tudo isso, pode-se dizer que, em geral, a Lei de Interceptações Telefôni-

cas contém dispositivos que pretendem garantir que a medida só venha a ser utilizada em casos em que elevado interesse público justifique o peso da restrição ao sigilo das comunicações.

Paralelamente, norma infralegal expedida pelo Conselho Nacional de Justiça, Resolução n. 59/08, regulamenta administrativamente o procedimento dos pedidos de interceptação, padroniza os termos de decisões judiciais sobre eles, define a forma de encaminhamento dos ofícios às empresas afetadas e responsabiliza os juízes a zelar pelo sigilo no tratamento das informações interceptadas. A Resolução n. 36/09 do Conselho Nacional do Ministério Público contém disposições semelhantes acerca das formas de pedido e de condução de interceptações. O objetivo de tais resoluções, que preenchem vazio legislativo, é limitar as possibilidades de abuso na concessão de ordens judiciais, diminuir riscos que comprometam o segredo e, assim, o sucesso de investigações, e aumentar a segurança no tratamento das informações interceptadas.

Ademais, as referidas resoluções preveem uma espécie de "controle" das interceptações em andamento por meio de relatórios a serem enviados para as autoridades competentes ou para os sistemas indicados. No caso dos membros do Ministério Público, conforme o art. 10 da Resolução 36/09 do CNMP, deverão informar mensalmente à Corregedoria-Geral "a quantidade de interceptações em andamento, bem como aquelas iniciadas e findas no período, além do número de linhas telefônicas interceptadas e de investigados que tiveram seus sigilos telefônico, telemático ou informático quebrados.". Em relação aos magistrados, o artigo 18 da Resolução nº 59/08 do CNJ, com redação atualizada pela Resolução nº 328 do mesmo órgão, determina a submissão das informações relativas aos pedidos de interceptação e as decisões de quebra de sigilo a serem adicionadas ao DataJud (Base Nacional de Dados do

Poder Judiciário). A partir destes dados, conforme a nova dinâmica estabelecida pela Resolução nº 328, haverá uma alimentação automática no SNCI (Sistema Nacional de Controle de Interceptação), e a partir disto, serão elaborados relatórios quantitativos disponíveis publicamente, respeitando-se os dispositivos da LGPD e instrumentos correlatos.

A PRÁTICA: CULTURA DE INTERCEPTAÇÕES

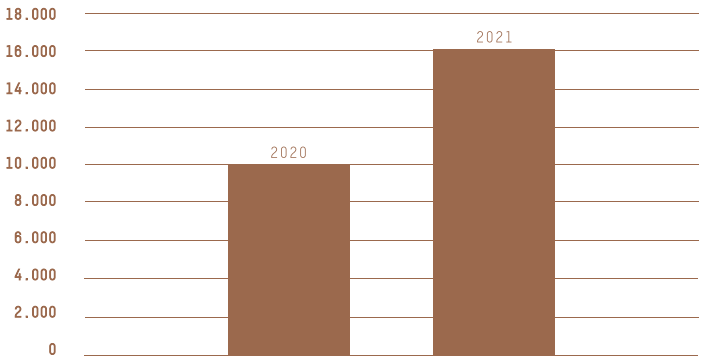
CASO ESCHER E OUTROS VS. BRASIL – CORTE INTERAMERICANA DE DIREITOS HUMANOS

O Brasil foi condenado pela Corte Interamericana de Direitos Humanos (CIDH), em julho de 2009, a indenizar trabalhadores rurais de cooperativas ligadas ao Movimento Sem-Terra, em razão de interceptações telefônicas irregulares realizadas no Estado do Paraná em 1999.[74] As interceptações, que duraram o total de 49 dias, foram autorizadas judicialmente em decisões não-fundamentadas, após requerimento de autoridade não-competente (Polícia Militar), fora do âmbito de uma investigação criminal corrente e sem notificação do Ministério Público, tudo em desrespeito à Lei das Interceptações Telefônicas. Além disso, trechos das interceptações que estavam sob segredo de justiça foram vazados e, a seguir, intencionalmente divulgados em coletiva de imprensa convocada pela Secretaria de Segurança Pública do Paraná dias após as gravações, também em desrespeito à Lei das Interceptações Telefônicas. Agravante foi, ainda, o fato de que as autoridades envolvidas nas interceptações ilegais não foram responsabilizadas em âmbito judicial interno brasileiro. Segundo a CIDH, o Brasil violou o direito à vida privada, à honra e à liberdade de associação das vítimas, além de violar garantias e proteções judiciais da Convenção Americana. As resoluções do CNJ e do CNMP vistas acima podem ser contextualizadas por este caso.

SISTEMA NACIONAL DE CONTROLE DE INTERCEPTAÇÕES

Em razão da Resolução nº 59/08 do Conselho Nacional de Justiça, juízes de varas criminais de todo o país são obrigados a adicionar informações processuais relativas aos pedidos de interceptações e às decisões de quebra de sigilo aos processos, que posteriormente serão adicionados ao DataJud (Base Nacional de Dados Processuais do Poder Judiciário), do qual se extrairão, automaticamente, os dados para alimentar o "Sistema Nacional de Controle de Interceptações" (SNCI), que recolhe informações sobre ofícios expedidos a prestadoras de serviço. A partir de 2020, com a vigência da Resolução nº 328 do CNJ, os dados são disponibilizados por meio de um painel acessível publicamente pelo site do CNJ.[75] As estatísticas listadas abaixo se referem às informações do SNCI em julho de 2022:

QUANTIDADE DE DECISÕES DE QUEBRA DE SIGILO TELEMÁTICO POR ANO



Embora o gráfico ilustre aparente crescimento na quantidade de decisões de quebra de sigilo em 2021, os dados de 2020 estão contabilizados pelo SNCI até julho, de tal forma que a quantidade prevista no painel não expressa o valor total de decisões daquele ano. Ademais, a metodologia de divulgação

dos dados mudou desde 2017. Anteriormente, os dados eram parametrizados por quantidade de telefones monitorados por mês. Hoje, o parâmetro de amostragem dos dados é a quantidade de decisões de quebra de sigilo telemático por ano. Dados anteriores ao ano de 2020 também não estão disponíveis no painel do SNCI, o que limita uma comparação acurada entre os diferentes anos desde a origem do sistema. Não é possível, assim, avaliar com precisão se houve retração ou aumento no número de pedidos de interceptação desde 2017.

Para dizer o que as estatísticas no SNCI representam em relação ao rigor com o qual a Lei de Interceptações Telefônicas tem sido aplicada pelo Poder Judiciário no Brasil, seria necessário ter acesso ao número total de pedidos de interceptações realizados ou, alternativamente, ao número de pedidos de interceptações que foram *indeferidos*, dados não informados pelo SNCI. Assim, não é possível saber a porcentagem de deferimentos, o que prejudica a constatação de um retrato completo sobre a cultura de interceptações no Brasil.

A título de comparação, sabe-se que o número referente a ordens de interceptações autorizadas *(authorized intercept orders)* nos Estados Unidos, país com população que supera a brasileira em aproximadamente 120 milhões, durante *todo o ano* de 2021, foi de 2.245.[76] No Brasil, o número é de 15.880 decisões que autorizaram interceptação no mesmo ano.

Ao analisar as estatísticas do SNCI, é preciso também trabalhar com a possibilidade de não revelarem a grandeza real da utilização de medidas de interceptação no país. A empresa Telefónica, que opera como Vivo no Brasil, divulga anualmente relatório de transparência que contém informações sobre pedidos que recebeu de autoridades estatais. Na parte do Brasil, informa que recebeu, em 2021, 291.429 requerimentos de interceptações de comunicações telefônicas e telemáticas.[77] Pelo que a empresa divulga, esse número faz referência à soma total de alvos (nú-

meros de telefone e conexões a Internet) que foram objeto de interceptação. Ainda assim, nota-se que, mesmo representando dados de uma só empresa do mercado de telecomunicações, tal número de requerimentos ultrapassa em quase 20 vezes o número total de decisões que autorizaram interceptação em 2021.[78]

Tudo isso aponta que os números relativos a interceptações no Brasil merecem um estudo próprio. Se se revelarem altos, podem sugerir, de um lado, que a proteção teórica pretendida pela necessidade de ordem judicial e pela previsão de requisitos mais rigorosos para realização desse procedimento na Lei de Interceptações não se reflete na prática. De outro, pode também apontar para deficiências estruturais nas capacidades investigativas da polícia judiciária, fazendo com que esta seja fortemente dependente desse meio agressivo de instrução probatória. Não são poucas as manifestações no sentido de que autoridades de segurança pública recorrem a medidas de interceptação e de quebra de sigilo como *prima ratio*.[79]

2.7. INFILTRAÇÕES DE AGENTES E COLETA DE DADOS

A disciplina da infiltração de agentes não é ainda exaustiva no Brasil. Para discernir o panorama normativo nacional, abordaremos a infiltrações por meio de invasões, e a coleta de dados de comunicações em redes sociais e aplicativos de mensagens e em fontes abertas.

INFILTRAÇÃO POR SOFTWARE: O ESTADO COMO HACKER

Em 2021, a empresa israelense "NSO Group" foi exposta por meio de uma lista "vazada" que levou a conhecimento do mundo o fato do aplicativo "Pegasus" secretamente espionar milhares de ativistas e jornalistas de todo o mundo. Seus principais clientes eram governos. O Brasil, ao que parece,

não chegou a adquirir o *software*, embora estejam registradas tratativas entre representantes brasileiros e a NSO, e tenha ganhado notoriedade a sua participação em um pregão eletrônico para a contratação de serviços de monitoramento de "dados abertos". A contratação do Pegasus encontrou obstáculos na opinião pública e em órgãos de controle, e o pregão acabou resultando na contratação de outro software substituto.[80] De fato, entendeu-se que tais ferramentas possuíam um escopo específico de alimentar uma "Abin paralela", uma entidade de inteligência não regulamentada, o que por si só é alarmante.[81]

O software é especialmente problemático, pois é capaz de explorar vulnerabilidades desconhecidas em aplicações e sistemas operacionais, de modo a permitir a tomada de controle do dispositivo. Não há, na legislação brasileira, norma que respalde o emprego deste e de outros softwares-espião para fins de segurança pública ou investigações criminais.

A utilização de *malware*, mesmo que dentro de investigação criminal com "interceptação" autorizada por ordem judicial, desperta preocupações que vão além do sigilo das comunicações e afetam a integridade das comunicações e sistemas e mesmo a cadeia de custódia da prova.[82] Tradicionalmente, interceptações reguladas pela Lei 9.296/96 dão acesso a informações contemporâneas, isto é, a ligações de certo número alvo a partir do momento em que se inicia a investigação, por um período limitado de dias. As invasões por *malware* são capazes de conceder acesso a dados armazenados por anos em dispositivos e a tudo o que se faz e se guarda em aplicativos instalados no aparelho, viabilizando ainda que o agente se substitua ao investigado, o que, considerando a economia digital e a importância cotidiana da Internet, majora o potencial de lesividade de tal conduta ao incrementar a extensão e a intensidade do poder de vigilância do Estado e compromete a confiabilidade da prova resultante.

"INFILTRAÇÃO" POR MEIO DE ESPELHAMENTO DE APLICATIVOS DE MENSAGEM: O PRECEDENTE FIRMADO PELO HABEAS CORPUS Nº 99735-SC

Em 2018, a Sexta Turma do STJ julgou o Recurso Ordinário em Habeas Corpus nº 99.735 - SC (2018/0153349-8), que teve por objeto a técnica de "espelhamento" de mensagens do WhatsApp.[83] O espelhamento é uma modalidade de utilização da mensageria WhatsApp oferecida pelo provedor da aplicação, e viabilizada através do sítio eletrônico, WhatsApp Web. Nessa modalidade, uma vez gerado e lido um Código QR (Quick Response), é viabilizado o acesso à conta através de mais de um dispositivo, o que implica a possibilidade de observação e a participação em todas as conversas, inclusive de envio e exclusão de mensagens enviadas ou recebidas pelo usuário.

A relatora, Ministra Laurita Vaz, afastou em seu voto a aplicação analógica dos dispositivos que regulam a interceptação telefônica, pela abrangência temporal, pela afetação potencial de todos os contatos do investigado, inclusive terceiros não alcançados pela investigação, e pela possibilidade da manipulação do conteúdo. Segundo a ministra, a ilegalidade da prova decorre dos próprios atributos da tecnologia, já que esta inviabiliza o rastreio de todos os atos da operação de coleta e a verificação de eventual adulteração de seu conteúdo.

AGENTES INFILTRADOS EM REDES SOCIAIS E APLICATIVOS DE MENSAGENS

Além de infiltrações por meio de programas eletrônicos de espionagem, há cada vez mais notícias de agentes policiais, militares e de inteligência infiltrados em redes sociais e aplicativos de mensagem. Nas duas caixas abaixo, apresentamos dois exemplos recentes de notícias nesse sentido. Como em

outras situações analisadas neste livro, a atuação desses agentes ocorre em uma zona cinzenta da lei.

A Lei das Organizações Criminosas autoriza, "em qualquer fase da persecução penal", a infiltração de *policiais* como meio de obtenção de prova em investigações contra organizações criminosas (art. 3º, VII). A medida só é admitida quando há indícios dessa infração penal, isto é, o enquadramento como *organização criminosa*, e a indispensabilidade do meio de prova (art. 10, §2º). Depende também de representação de delegado de polícia ou requerimento do Ministério Público e de autorização judicial, que impõe os seus limites (art. 10, caput). Os pedidos devem demonstrar a necessidade da medida, o alcance das tarefas dos agentes e, quando possível, os nomes dos investigados e o local da infiltração (art. 11). A Lei 11.343/2006 também prevê a infiltração policial no art. 53, para os crimes relacionados ao comércio ilegal de entorpecentes.

Desde 2017, o Estatuto da Criança e do Adolescente (Lei nº 8.069/1990) prevê a infiltração de agentes de polícia *na internet*, no art. 190-A, como medida de investigação nos crimes contra as crianças e adolescentes previstos na lei, desde que haja ordem judicial, a medida seja delimitada em seu escopo e tempo (dois anos), seja demonstrada sua necessidade, e se elabore relatório circunstanciado. Mais recentemente, as infiltrações virtuais de agentes policiais também foram previstas para a obtenção de provas em investigações contra organizações criminosas, segundo uma nova redação da Lei das Organizações Criminosas nos termos da Lei 13.964/2019.

A lei disciplina as hipóteses de infiltrações virtuais, seus procedimentos, condições e prazos. Tais medidas se referem a infiltrações de agentes policiais e abrangem o engajamento desses agentes em redes sociais e mesmo espaços privados.

2.8. ACESSO A DADOS SEM TRANSPARÊNCIA PARA FINS DE INTELIGÊNCIA E SEGURANÇA NACIONAL

A ABRANGÊNCIA DO SISBIN

A Lei nº 9.883/99 instituiu o Sistema Brasileiro de Inteligência (SISBIN), que integra ações de planejamento e execução de tarefas de inteligência no Brasil, com a finalidade de fornecer à Presidência da República subsídios nos assuntos de interesse nacional, pela obtenção, análise e disseminação de conhecimentos relevantes à ação e processo decisório governamentais e garantia da segurança da sociedade e do Estado (art. 1º). Compõem o Sisbin todos os órgãos da Administração Pública Federal que possam produzir conhecimentos de interesse das atividades de inteligência (art. 2º). A relação de órgãos consta no art. 4º do Decreto nº 4.376/02, que reúne a Casa Civil e o Gabinete de Segurança Institucional da Presidência da República, os Ministérios da Justiça e Segurança Pública; da Defesa; das Relações Exteriores; da Economia; da Fazenda; da Infraestrutura; da Educação; da Saúde; das Comunicações; da Ciência, Tecnologia e Inovações; da Mulher, da Família e dos Direitos Humanos; da Agricultura, Pecuária e Abastecimento; do Meio Ambiente; do Desenvolvimento Regional, além do Banco Central do Brasil. A lista compreende ainda órgãos relacionados a estes ministérios como a Diretoria de Inteligência da Polícia Federal e da Polícia Rodoviária Federal, o Departamento Penitenciário Nacional, o Departamento de Cooperação Jurídica Internacional, o Centro de Inteligência das Forças Armadas e a Receita Federal. A Agência Brasileira de Inteligência (ABIN) constitui o órgão central do sistema e tem por atribuição planejar e executar as atividades de inteligência. A Política Nacional de Inteligência, sancionada pelo decreto presidencial nº 8.793 de 29 de junho de 2016, orienta

as atividades de inteligência no Brasil e define os "parâmetros e limites de atuação da atividade de Inteligência e de seus executores e estabelece seus pressupostos, objetivos, instrumentos e diretrizes, no âmbito do Sistema Brasileiro de Inteligência (SISBIN)".

A Lei nº 9.883/99 estabelece que os órgãos do Sisbin fornecerão à ABIN dados e conhecimentos específicos relacionados com a defesa das instituições e dos interesses nacionais (Art. 4º, parágrafo único). O art. 6, inciso V do Decreto 4.376/02, que regulamentou o funcionamento do SISBIN, dispõe que cabe aos órgãos desse sistema intercambiar e fornecer informações necessárias à produção de conhecimentos para as atividades de inteligência. O art. 6-A do mesmo Decreto, conforme redação dada em 2021 (Decreto 10.759/2021), previu que a ABIN poderá requerer e manter representantes de órgãos do SISBIN junto a seu Centro de Inteligência Nacional, os quais, a despeito de estarem dispensados do exercício das atribuições no órgão de origem, "poderão acessar, por meio eletrônico, as bases de dados de seus órgãos de origem, respeitadas as normas e limites de cada instituição e as normas legais pertinentes à segurança, ao sigilo profissional e à salvaguarda de assuntos sigilosos" (§ 4º). A Política Nacional de Inteligência, publicada em 2016, através do Decreto nº 8.793/2016, também estabelece como diretriz do SISBIN o "compartilhamento de dados e conhecimentos" entre os diversos organismos estatais.[84] Em dezembro de 2017, foi editada a Estratégia Nacional de Inteligência, seguida, em maio de 2018, pelo Plano Nacional de Inteligência. Mais recentemente, o Decreto 10.445/2020 estabeleceu a estrutura regimental.

Em tese, portanto, seria possível à ABIN ter acesso a informações e dados a princípio protegidos pelo sigilo das comunicações, a despeito de não poder realizar diretamente interceptações, por não ter sido contemplado o fim de inteligência na Constituição nem na Lei das Interceptações.[85] Tal

interpretação chegou a dar ensejo a episódios como o revelado pelo jornal *Folha de São Paulo* em 2008, no qual se constatou acesso indireto da ABIN a comunicações interceptadas disponíveis no sistema Guardião da Polícia Federal.[86]

Mais recentemente, no entanto, o Supremo Tribunal Federal determinou, ao julgar a ADI 6529, que o fornecimento de dados estará condicionado à existência de interesse público, que as solicitações de dados deverão ser formalmente motivadas, habilitando posterior controle judicial, e que informações protegidas por sigilo, como comunicações telefônicas ou de dados, não poderão ser compartilhadas. Estabeleceu ainda a necessidade de instauração formal de procedimento e de emprego de sistemas de segurança e registro de acesso, para fins de controle e eventual responsabilização.[87]

Cumpre notar que, embora a LGPD não se aplique a tratamentos de dados pessoais realizado para fins exclusivos de defesa nacional e segurança do Estado (art. 4º, III, b, c), por força do art. 5º, LXXIX da CF e do art. 4º, § 1º da Lei 13.709/ 2018, tais atividades ainda estarão submetidas aos princípios gerais de proteção e aos direitos do titular. Além disso, pela Lei 9.883/99, o Sisbin, em geral, e a ABIN, em particular, estão obrigados a respeitar direitos e garantias constitucionais em sua atuação (art. 1º, § 1º e art. 3º, parágrafo único), que é controlada e fiscalizada externamente pela Comissão Mista de Controle das Atividades de Inteligência, comissão permanente do Congresso Nacional (art. 6º). A falta de transparência sobre a forma como se dá a cooperação pelo SISBIN impede, contudo, a avaliação rigorosa da ABIN em termos de vigilância, e cobre a sua atuação de obscuridade e incertezas.

/ 3. RECOMENDAÇÕES E BOAS PRÁTICAS NA PERSPECTIVA INTERNACIONAL /

O presente livro apresentou leis e práticas brasileiras de vigilância das comunicações. Diante deste panorama e tomando como referência os 13 Princípios Internacionais sobre a Aplicação de Direitos Humanos à Vigilância das Comunicações, elaborados por uma coalizão global de especialistas em privacidade e tecnologia da sociedade civil,[88] apresentamos as recomendações a seguir.

LEGALIDADE: Os limites do direito à privacidade devem ser definidos clara e precisamente em leis, e devem ser regularmente revistos para garantir que as proteções à privacidade prossigam lado a lado com as rápidas mudanças tecnológicas.

FIM LEGÍTIMO: A vigilância das comunicações só deve ser permitida em busca dos objetivos mais importantes do Estado.

NECESSIDADE: O Estado tem a obrigação de provar que suas atividades de vigilância das comunicações são necessárias para alcançar um objetivo legítimo.

ADEQUAÇÃO: Um mecanismo de vigilância das comunicações deve alcançar seu objetivo legítimo efetivamente.

PROPORCIONALIDADE: A vigilância de comunicações deve ser considerada como um ato altamente intrusivo que interfere nos direitos à privacidade e na liberdade de expressão e opinião, ameaçando os fundamentos de uma sociedade democrática. A vigilância proporcional vai tipicamente requerer uma autorização prévia de uma autoridade judicial competente.

AUTORIDADE JUDICIAL COMPETENTE: Determinações relativas à vigilância de comunicações devem ser expedidas por uma autoridade judicial competente que seja imparcial e independente.

DEVIDO PROCESSO LEGAL: O devido processo legal requer que qualquer interferência com os direitos humanos seja governada por procedimentos legais, publicamente disponíveis e aplicados consistentemente em uma audiência pública e justa.

NOTIFICAÇÃO DO USUÁRIO: Os indivíduos devem ser notificados de uma decisão autorizando a vigilância de suas comunicações. Exceto quando uma autoridade judicial competente conclua que

um aviso prejudicaria a investigação, os indivíduos devem ter uma oportunidade de questionar tal vigilância antes que ela ocorra.

TRANSPARÊNCIA: O governo tem a obrigação de tornar públicas informações suficientes para que o público em geral possa entender o escopo e a natureza de suas atividades de vigilância. O governo não deve impedir, de um modo geral, que os provedores de serviço publiquem detalhes sobre o escopo e a natureza de seus próprios acordos de vigilância feitos com o Estado.

ESCRUTÍNIO PÚBLICO: Estados devem estabelecer mecanismos de fiscalização para garantir a transparência e responsabilização da vigilância de comunicações. Os órgãos de controle devem ter a autoridade para acessar todas as informações relevantes a respeito das ações do Estado.

INTEGRIDADE DAS COMUNICAÇÕES E SISTEMAS: Os provedores de serviço e produtores de hardware ou software não podem ser compelidos a embutir capacidades de vigilância ou monitoramento em seus sistemas, coletar ou reter informação particular apenas para fins de vigilância estatal.

SALVAGUARDAS PARA A COOPERAÇÃO INTERNACIONAL: Ocasionalmente, os Estados podem precisar da assistência de provedores de serviço estrangeiros para conduzir vigilância. Isso deve ser governado por tratados claros e públicos, que garantam que os standards de maior proteção à privacidade sejam aplicados.

SALVAGUARDAS CONTRA O ACESSO ILEGÍTIMO: Deve haver penalidades, nas esferas civil e criminal, impostas a qualquer parte responsável por vigilância ilegal e aqueles afetados por mecanismos de vigilância devem ter acesso a remédios jurídicos efetivos. Também deve ser garantida a proteção daqueles que denunciam atividades de vigilância que afetam direitos humanos.

/ 4. CONSIDERAÇÕES FINAIS /

Cinco anos após o lançamento da segunda edição deste estudo, percebe-se que algumas questões ainda se mantêm. Um dos problemas básicos identificados, assim, segue sendo a adoção de interpretações restritivas dadas a direitos fundamentais da Constituição brasileira, que ameaçam, na prática, a efetividade da proteção que esses direitos garantem. Há avanços na legislação brasileira sobre proteção de dados que devem ser reconhecidos, como a entrada em vigor da Lei Geral de Proteção de Dados e o reconhecimento do direito à proteção de dados como direito fundamental. Apesar disso, ainda há lacunas importantes em relação às possibilidades de uso e acesso a dados no âmbito da segurança pública e persecução penal.

Atualmente, tramitam no STF diferentes ações que se relacionam com as divergências interpretativas exploradas ao longo deste relatório. Especificamente, chamamos a atenção para *(i)* a ADI 5063/DF, que contesta a constitucionalidade dos arts. 15 (acesso a dados cadastrais por autoridade policial e Ministério Público por mera requisição), 17 (obrigação de guarda de registros telefônicos) e 21 (criminalização da recusa ao acesso) da Lei das Organizações Criminosas; *(ii)* a ADI 4906, que contesta o art. 17-B (acesso a dados cadastrais por autoridade policial e Ministério Público por mera requisição) da Lei dos Crimes de Lavagem de Dinheiro; e *(iii)* a ADI 5642, que contesta a constitucionalidade dos arts. 13-A (acesso a dados cadastrais por delegados e Ministério Público por mera requisição em casos relacionados a tráfico de pessoas) e 13-B (acesso a "sinais", excepcionalmente mesmo sem ordem judicial) do Código de Processo Penal.

A Lei das Organizações Criminosas fere diversos princípios internacionais: legalidade (não é clara em nenhum de seus termos), necessidade (institui guarda de registros telefônicos por 5 anos sem estar amparada por evidência empírica da necessidade), proporcionalidade (não restringe expressamente as hipóteses de acesso aos registros guardados; impõe pena de reclusão

e multa à recusa de acesso a dados), autoridade judicial competente (permite interpretações abrangentes quanto aos dados que podem ser exigidos sem ordem judicial) e notificação do usuário (não contém previsões quanto a isso). A Lei dos Crimes de Lavagem de Dinheiro e as adições ao Código de Processo Penal padecem de problemas semelhantes. Ações que contestam a constitucionalidade dessas leis enfrentarão, no mínimo, as questões sobre a necessidade e proporcionalidade da obrigação de guarda de registros telefônicos e a abrangência das possibilidades de acesso a dados por autoridades competentes sem ordem judicial. Em razão disso, o julgamento da constitucionalidade dessas leis estabelecerá precedentes importantes sobre a proteção à privacidade e ao sigilo das comunicações no Brasil.

O acesso a registros telefônicos e outros metadados possui tratamento improvisado na Lei das Organizações Criminosas. O acesso a metadados no Brasil precisaria, idealmente, de regulamento próprio: uma lei que contenha requisitos claros de acesso (formais, prevendo-se nomeadamente as autoridades competentes para fazerem pedidos e estipulando a necessidade de ordem judicial; e materiais, restringindo-os para certos tipos de processos e exigindo fundamentação razoável), regras de notificação do usuário e de transparência sobre quantidade de pedidos. Os casos em que o pedido de quebra se refira a dados sobre a localização do usuário precisaria ser diferenciado daquele em que o pedido se refere a registros telefônicos. Se impusesse vigilância obrigando a guarda de dados, como fez a Lei das Organizações Criminosas, uma tal lei deveria ser também no mínimo clara sobre dados a serem guardados, período, respeitados os princípios da necessidade e da proporcionalidade, e conter normas de segurança para guarda de dados.

Reformas legislativas conferiram poderes de acesso por mera requisição a dados cadastrais de usuários de telefonia a autoridades policiais e ao Ministério Público e outros projetos

de lei em andamento pretendem estender essas possibilidades de acesso direto também a dados cadastrais de usuários da Internet e a metadados. Isso parece sugerir que *(i)* a investigação criminal no Brasil é fortemente dependente de quebras de sigilo de dados cadastrais e de metadados, na falta de infraestrutura e pessoal para utilização de métodos de investigação ou da deficiência dos existentes; e/ou *(ii)* a morosidade do sistema judiciário brasileiro tem sido contornada por autoridades envolvidas em atividades investigativas, por meio de pressão por alterações legislativas que facilitem o acesso a dados. Nos dois casos, perdem os direitos fundamentais ao sigilo das comunicações, à privacidade e à liberdade de expressão. A realização de estudos empíricos sobre práticas de requisição de dados cadastrais e de metadados, colhendo-se números sobre quantidades de pedidos e realizando-se entrevistas com agentes envolvidos, poderá indicar razões reais desse panorama e indicar caminhos para a sua solução, dando conta de todos os interesses em jogo.

O Marco Civil da Internet contém direitos e garantias importantes que protegem o usuário da rede contra vigilância indevida de suas comunicações, principalmente por conter requisitos claros sobre as hipóteses e requisitos de acesso a registros de conexão à Internet, de acesso a aplicações e a comunicações privadas armazenadas. Está de acordo com o princípio da legalidade e da autoridade judicial competente.

Apesar disso, o art. 15 do Marco Civil da Internet, que institui a obrigação de guarda de registros de acesso a aplicações, precisa ter seus termos revistos. Os dados a que se referem essa obrigação são capazes de revelar informações de forte impacto à privacidade dos usuários na rede, uma vez que se referem ao próprio comportamento virtual do usuário, podendo revelar seus interesses, hábitos e contatos. A existência de meios menos graves de restrição a direitos fundamentais – como a hipótese de ordenar a guarda de dados apenas após suspeita

(indícios de autoria e participação em crime) – e que atingem os mesmos fins de eficácia em investigações colocam dúvidas sobre a necessidade dessa medida. Diante disso, deve-se considerar a restrição das hipóteses de acesso a esses dados apenas para a esfera penal, para crimes graves cometidos pela Internet, com previsões específicas, a redução do tempo e dos destinatários da guarda apenas ao estritamente necessário, o que aproximaria a previsão de uma restrição proporcional à privacidade e ao sigilo das comunicações.

Frequentemente, a resistência de provedores de aplicações de Internet a fornecer dados de usuários (principalmente conteúdo) a autoridades brasileiras, sobretudo as judiciais, é encarada como afronte à sua autoridade ou à soberania nacional. Nesse contexto, as tensões envolvendo autoridades e empresas podem assumir contornos radicais, como medidas de bloqueios de aplicativos.

Como exposto neste livro, os acordos internacionais de cooperação mútua em matéria penal são instrumentos que podem servir como uma via mais diplomática para o equacionamento dessas tensões. Por diferentes razões, contudo, a utilização desses acordos para a obtenção de provas no contexto da Internet enfrenta uma série de obstáculos, o que acabou estigmatizando-os como uma solução ineficiente para as necessidades das autoridades. Para atender às necessidades de autoridades e ao mesmo tempo garantir o respeito a direitos humanos como a privacidade e a liberdade de expressão, é necessário rever e atualizar esses arranjos em vez de simplesmente abandoná-los. Isso exige debate público sobre qual a melhor forma de torná-los mais céleres e eficientes, o que passa por identificar seus principais gargalos e deficiências e analisar as suas alternativas de melhoria.

O estudo também mostrou que a Lei das Interceptações Telefônicas se aplica não só a interceptações telefônicas, mas também às telemáticas. Mais que isso, também indicou que

tem-se buscado estender a aplicação da Lei para novos casos como o da infecção de *malware* em celulares e computadores. Isso está em desacordo com o princípio da legalidade e precisa ser revisto: este tipo de tecnologia não só quebra o sigilo das comunicações, restringido pela Lei das Interceptações, mas impõe novas questões acerca da proteção à integridade e confidencialidade de sistemas, merecendo regramento próprio.

Por fim, pouco se estuda a atuação da ABIN e do SISBIN no Brasil. Do controle exercido pela Comissão Mista do Congresso Nacional também quase não se tem notícia. O programa que a ABIN usa para monitorar comunicações públicas – e que ganhou relevância com os grandes eventos ocorridos no Brasil – é o máximo do que se ficou sabendo. Recomendação básica parece ser prestar atenção nesses órgãos, exigindo transparência sobre a sua atuação, para que avaliações completas sobre eles possam ser feitas e, assim, o escrutínio público seja possibilitado.

Quando se diz neste livro que a ABIN não faz interceptações, que é o que manda a lei, diz a jurisprudência e afirma a ABIN, é quase difícil acreditar: o Brasil possui uma autoridade de segurança nacional que não faz interceptações de comunicações, uma autoridade de vigilância que não vigia. Parece que essa impossibilidade é, ou pelo menos pode ser, contornada pelo SISBIN. Diante disso, para que se observem princípios internacionais em matéria de vigilância, é fundamental que haja transparência sobre a atuação da agência e, principalmente, sobre a forma como a cooperação entre SISBIN e outros órgãos, como a Polícia Federal e a Receita Federal, ocorre. Balizas precisam ser criadas para as possibilidades dessa cooperação, uma vez que a finalidade de dados recolhidos sobre comunicações – pela Polícia Federal, em nome de fins investigatórios criminais; pela Receita Federal, em nome de fins fiscalizatórios tributários – pode estar sendo desvirtuada para a sua utilização para fins de inteligência.

/ NOTAS /

1. ABREU, Jacqueline de Souza; ANTONIALLI, Dennys. "Vigilância das comunicaçõespelo estado brasileiro e a proteção a direitos fundamentais". São Paulo: InternetLab,2015, disponível em: http://www.internetlab.org.br/wp-content/uploads/2016/01/ILAB_Vigilancia_Entrega_v2-1.pdf. Acesso: 06.05.2017; ABREU, Jacqueline de Souza; ANTONIALLI, Dennys. "Vigilância sobre as comunicações no Brasil". São Paulo: InternetLab, 2017. disponível em: http://www.internetlab.org.br/wp-content/uploads/2017/05/Vigilancia_sobre_as_comunicacoes_no_Brasil_2017_InternetLab.pdf. Acesso: 02.08.2022.

2. Os princípios foram elaborados pela EFF em esforço de fornecer uma estrutura para avaliar se as leis e práticas de vigilância atuais ou propostas são consistentes com os direitos humanos, e são resultado de consulta feita com grupos da sociedade civil, indústria e especialistas no tema. Para maiores informações, ver: https://necessaryandproportionate.org/

3. No que se refere à proteção do *fluxo* de comunicações, paradigmático é o texto FERRAZ JR., Tercio Sampaio, Sigilo de Dados: o direito à privacidade e os limites da função fiscalizadora do Estado, in: *Revista da Faculdade de Direito da Universidade de São Paulo*, v. 88, 1993, p. 439-459. No que se refere à aplicação da exceção, concordam SILVA, José Afonso da. *Curso de Direito Constitucional Positivo*. 32ª Ed. São Paulo: Malheiros, 2008, p. 438; e FERREIRA FILHO, Manoel Gonçalves. *Curso de Direito Constitucional*. 35ª Ed. São Paulo: Saraiva, 2009, p. 301.

4. No julgamento do Recurso Extraordinário 418.416-8/SC, de 10/05/2006, o Min. Rel. Sepúlveda Pertence afirma que a proteção do inciso XII do art. 5º não se refere às informações comunicadas em correspondências, mensagens telegráficas, dados e telefonemas em si, mas à comunicação, ao *fluxo* das mesmas enquanto ocorrem. Implicitamente, também exclui a aplicação da exceção prevista na letra do inciso XII do art. 5 ao fluxo de dados.

5. SUPREMO TRIBUNAL FEDERAL. Habeas Corpus 168.052 São Paulo. Ministro Gilmar Mendes, julgado em 20.10.2020. Disponível em: downloadPeca.asp (stf.jus.br)

6. Ver, por exemplo, SUPREMO TRIBUNAL FEDERAL. Mandado de Segurança 24.817/DF, Min. Celso de Mello, julg. em 03.02.2005, que associa quebras de sigilo de fiscal, bancário e telefônico a restrições ao art. 5, X. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=2205427. Acesso em: 17.06.2015. Na doutrina, ver, por exemplo, BADARÓ, Gustavo Henrique Righi Ivahy. "Interceptação de comunicações telefônicas e telemáticas: limites ante o avanço da tecnologia". In: LIMA, José Corrêa de; CASARA, R. R. Rubens. (coord.). *Temas para uma perspectiva crítica do direito: homenagem ao Professor Geraldo Prado*. Rio de Janeiro: Lumen Juris, 2010, pp. 483-499, p. 485.

7. Alterações legislativas "contornam" necessidade de ordem judicial para obtenção de dados cadastrais, como se verá adiante neste relatório (item "Vigilância *sem* e *com*

contrapesos: Telefonia vs. Internet"), desrespeitando entendimento já apresentado pelo Supremo Tribunal Federal. Ver SUPREMO TRIBUNAL FEDERAL, Recurso Extraordinário 716795/RS, Min. rel. Luiz Fux, julg. 31.10.2012, sobre a discussão acerca da exigência de autorização judicial para obtenção de dados cadastrais de usuários de telefonia por parte de delegados de polícia, concluindo pela necessidade dela por estar protegidas pelo art. 5, X. Disponível em: http://stf.jusbrasil.com.br/jurisprudencia/22599582/recurso-extraordinario-re-716795-rs-stf. Acesso em: 17.06.2015.

8. Ver ANTONIALLI, Dennys; BRITO CRUZ, Francisco; VALENTE, Mariana Giorgetti, "*Smartphones*: baús de tesouro da Lava Jato", *Deu nos Autos*, 24 de novembro de 2016, disponível em: http://link.estadao.com.br/blogs/deu-nos-autos/smartphones-baus-do-tesouro-da-lava-jato/. Acesso em: 20.01.2017 (comentando decisão do Superior Tribunal de Justiça que concluiu pela desnecessidade de ordens judiciais específicas para acesso a informações armazenadas em smartphones apreendidos mediante mandados de busca e apreensão); MARANHÃO, Juliano,"O acesso ao WhatsApp pela operação Lava Jato", *Jota*, disponível em: http://jota.info/artigos/o-acesso-ao-whatsapp-pela-operacao-lava-jato-05122016. Acesso em: 20.01.2017.

9. Neste sentido, ver SIDI, Ricardo, A interceptação de e-mails e a apreensão física de e-mails armazenados, *Revista Fórum de Ciências Criminais*, n.4, pp. 101-21 julho/dezembro 2015, pp. 111-8.

10. SUPERIOR TRIBUNAL DE JUSTIÇA. Agravo Regimental no Agravo em Recurso Especial nº 1.910.871/RS. Ministro Reynaldo Soares da Fonseca, julgado em 19.10.2021. Disponível em: https://processo.stj.jus.br/processo/pesquisa/?tipoPesquisa=tipoPesquisaNumeroRegistro&termo=202101900191&totalRegistrosPorPagina=40&aplicacao=processos.ea

11. SUPERIOR TRIBUNAL DE JUSTIÇA. Recurso em Habeas Corpus nº 75.800-PR. Ministro Felix Fischer, julgado em 15.09.2016. Disponível em: http://www.internetlab.org.br/wp-content/uploads/2016/11/lavajato.pdf. A decisão foi comentada criticamente em ANTONIALLI, Dennys; BRITO CRUZ, Francisco; VALENTE, Mariana Giorgetti, "*Smartphones*: baús de tesouro da Lava Jato", *Deu nos Autos*, 24 de novembro de 2016. Disponível em: http://link.estadao.com.br/blogs/deu-nos-autos/smartphones-baus-do-tesouro-da-lava-jato/. Acesso em: 20.01.2017.

12 O julgamento do tema teve início em 2020, com voto do relator Ministro Dias Toffoli pelo provimento do Recurso Extraordinário e pela licitude da prova obtida nos termos do tema de repercussão geral. No entanto, o Ministro Gilmar Mendes e Edson Fachin divergiram da posição do relator para fixar a seguinte tese: "O acesso a registro telefônico, agenda de contatos e demais dados contidos em aparelhos celulares apreendidos no local do crime atribuído ao acusado depende de prévia decisão judicial que justifique, com base em elementos concretos, a necessidade e a adequação da medida e delimite a sua abrangência à luz dos direitos fundamentais à intimidade, à privacidade e ao sigilo das comunicações e dados dos indivíduos

(CF, art. 5º, X e XX)". O Ministro Alexandre de Moraes pediu vista dos autos, suspendendo o julgamento, que já foi incluído para continuar no dia 18 de agosto de 2022

13. SUPREMO TRIBUNAL FEDERAL. Habeas Corpus 168.052/ SP. Min. Gilmar Mendes, julg. 20.10.2020. Disponível em: downloadPeca.asp (stf.jus.br)

14. SUPREMO TRIBUNAL FEDERAL. Habeas Corpus nº 91.867/SP. Min. rel. Gilmar Mendes, julg. 24.04.2012.

15. SUPERIOR TRIBUNAL DE JUSTIÇA. Habeas Corpus nº 66.368/PA. Min. rel. Gilson Dipp, 5ª Turma, julg. 05.06.2007.

16. SUPERIOR TRIBUNAL DE JUSTIÇA. Habeas Corpus n. 372.762/MG. Ministro Felix Fischer. Julgado em 3.10.2017.

17. SUPERIOR TRIBUNAL DE JUSTIÇA. Recurso Especial 1.782.386/RJ. Julgado em 15.12.2020. Disponível em: https://processo.stj.jus.br/processo/pesquisa/?tipoPesquisa=tipoPesquisaNumeroRegistro&termo=201803152161&totalRegistrosPorPagina=40&aplicacao=processos.ea.

18. SUPERIOR TRIBUNAL DE JUSTIÇA. Recurso Ordinário em Habeas Corpus nº 51.531/RO. Min. rel. Nefi Cordeiro. 6ª Turma, julg. 19.04.2016.

19. ANTONIALLI, Dennys, *et al*. Acesso de autoridades policiais a Celulares em abordagens e flagrantes: retrato e análise da jurisprudência de tribunais estaduais. Revista Brasileira de Ciências Criminais | vol. 154/2019 | p. 177 - 214 | Abr / 2019.

20. Ver, sobre o tema, LOPES JR., Aury. *Direito Processual Penal*. 13ª Ed. São Paulo: Saraiva, 2016, p. 616; BADARÓ, Gustavo Henrique. *Direito Processual Penal*. Tomo II. 2ª Ed. Rio de Janeiro: Elsevier, 2009, p. 185.

21. Ver, por exemplo, argumento neste sentido em GARCIA, Rafael de Deus, "Acesso a dados em celular exige ordem judicial", *Consultor Jurídico*, 06 de fevereiro de 2017, disponível em: https://www.conjur.com.br/2017-fev-06/rafael-garcia-acesso-dados-celular-exige-autorizacao-judicial.

22. Ver, por exemplo, argumento neste sentido em BARRETO, Alesandro Gonçalves; FERRER, Everton Ferreira de Almeida, "Perícia em celular: necessidade de ordem judicial?", *Direito & TI*, 04 de junho de 2016, disponível em: https://direitoeti.emnuvens.com.br/direitoeti/article/view/52. Acesso em: 05.05.2017.

23. Ver, sobre isso, ABREU, Jacqueline de Souza, "From Jurisdictional Battles to Crypto Wars: Brazilian Courts v. WhatsApp", *Columbia Journal of Transnational Law Online*

Edition, 17 de outubro de 2016, disponível em: http://jtl.columbia.edu/from-jurisdictional-battles-to-crypto-wars-brazilian-courts-v-whatsapp/. Acesso em: 20.01.2017.

24. "MPF investiga se a criptografia do WhatsApp permite a quebra de sigilo por autoridades judiciais", Notícias do MPF em Mato Grosso, 03 de maio de 2016, disponível em http://www.mpf.mp.br/mt/sala-de-imprensa/noticias-mt/mpf-investiga-se-a-criptografia-do-whatsapp-permite-a-quebra-de-sigilo-por-parte-das-autoridades-judiciais-do-pais.

25. FERRAZ JR., Tercio Sampaio; MARANHÃO, Juliano; FINGER, Marcelo. "O desafio do WhatsApp ao Leviatã", *Folha de São Paulo*, 16 de agosto de 2016, disponível em http://www1.folha.uol.com.br/opiniao/2016/08/1803323-o-desafio-do-whatsapp-ao-leviata.shtml. Acesso em: 08.05.2017.

26. "Governo elabora projeto para regular acesso a informações do WhatsApp, G1, 19 de julho de 2016, disponível em https://portal.stf.jus.br/processos/detalhe.asp?incidente=2205427. Acesso em: 08.05.2017.

27. Ver BARROS, Paula Pécora de. "ADPF 403 no STF: Bloqueios do WhatsApp são constitucionais?" In: bloqueios.info, InternetLab, 18 de novembro de 2016, disponível em: http://bloqueios.info/pt/adpf-403-no-stf-bloqueios-do-whatsapp-sao-constitucionais/. Acesso em: 08.05.2017.

28. SUPREMO TRIBUNAL FEDERAL. Relatores consideram inconstitucional quebra do sigilo de comunicação em aplicativos de mensagens. 2020. Disponível em: Supremo Tribunal Federal (stf.jus.br).

29. ABREU, Jacqueline de Souza; ANTONIALLI, Dennys, Vigilância das Comunicações pelo Estado Brasileiro FAQ, *Necessary & Proportionate*, 2016, disponível em: https://necessaryandproportionate.org/pt/vigilância-das-comunicações-pelo-estado-brasileiro-faq. Acesso em: 08.05.2017.

30. O InternetLab perguntou à ANATEL, via Lei de Acesso à Informação, que tipos de informações fazem parte de "documentos fiscais". A resposta aponta para todas as informações constantes em faturas de clientes. "Quando a fiscalização tem objetivo investigar possíveis práticas de cobranças indevidas por parte da operadora, se houve ou não ressarcimento aos usuários em casos de interrupção do serviço ou outras situações envolvendo faturamento dos serviços, pode ser necessário obter das operadoras um conjunto de amostras de faturas enviadas aos consumidores, escolhidos aleatoriamente, com o propósito de verificar se as práticas investigadas estão afetando os usuários dos serviços de forma generalizada."

31. A extrapolação da competência da ANATEL em matéria de retenção de dados foi investigada, olhando-se para as tramitações de suas resoluções, em ABREU,

Jacqueline de Souza, "Guarda obrigatória de registros de telecomunicações no Brasil: sobre as origens da retenção de dados e as perspectivas para direitos fundamentais", Anais do IV Simpósio Internacional LAVITS, 2017, no prelo.

32. Sobre isso, ver VARON FERRAZ, Joana., Boletim n. 11 da Oficina Antivigilância, disponível em https://antivigilancia.org/pt/2015/07/novas-revelacoes-do-wikileaks-sobre-vigilancia-no-brasil-dilma-disse-que-nao-tem/. Refere-se a acordo disponível em https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/atos-assinados-por-ocasiao-da-visita-da-presidenta-dilma-rousseff-aos-estados-unidos-washington-30-de-junho-de-201. Acesso em: 31.07.2015.

33. Paralelamente, a Lei nº 12.830/2013 também instituiu no seu art. 2, §2º, que "durante a investigação policial, cabe ao delegado de polícia a requisição de perícia, informações, documentos e dados que interessem à apuração dos fatos".

34. Esse entendimento chegou a ser acolhido pelo Supremo Tribunal Federal. Ver SUPREMO TRIBUNAL FEDERAL, Recurso Extraordinário 716795/RS, Min. rel. Luiz Fux, julg. 31.10.2012, em que se discute a exigência de autorização judicial para obtenção de dados cadastrais de usuários de telefonia por parte de delegados de polícia, concluindo pela necessidade dela. Disponível em: https://portal.stf.jus.br/processos/detalhe.asp?incidente=4313899.

35. TRIBUNAL REGIONAL FEDERAL 3ª REGIÃO. Apelação/Reexame Necessário nº 0000108-56.2013.4.03.6110/SP. Rel. Des. Johonson di Salvo, julg. 03.03.2016. Disponível em: http://web.trf3.jus.br/acordaos/Acordao/BuscarDocumentoGedpro/4976979 . Acesso em 17.01.2017. A decisão modificou sentença de primeira instância em favor da Claro.

36. Ver, nesse sentido, ARAS, Vladimir, "A investigação criminal na nova lei de lavagem de dinheiro", *Boletim 237 do IBCCRIM*, disponível em: http://www.ibccrim.org.br/boletim_artigo/4671-A-investigao-criminal-na-nova-lei-de-lavagem-de-dinheiro. Acesso em: 17.06.2015; BARBOSA, Júlia de Carvalho, "O sigilo de dados cadastrais dos clientes de empresas telefônicas", *Conteúdo Jurídico*, 22 de abril de 2014, disponível em: https://www.conteudojuridico.com.br/consulta/Artigos/39000/o-sigilo-de-dados-cadastrais-dos-clientes-de-empresas-telefonicas. Acesso em: 17.01.2017.

37. A petição da ACEL e exemplos de intimações recebidas por operadoras com base nessa (interpretação da) lei podem ser encontradas em CONJUR, "Operadoras reclamam de pedidos de delegados para quebra de sigilo telefônico", 29 de outubro de 2014, disponível https://www.conjur.com.br/2014-out-29/telefonicas-reclamam-quebras-sigilo-pedidas-delegados#:~:text=Operadoras%20reclamam%20de%20pedidos%20de%20delegados%20para%20quebra%20de%20

sigilo%20telef%C3%B4nico&text=As%20operadoras%20de%20telecomunica%-C3%A7%C3%B5es%20brasileiras,que%20trata%20de%20organiza%C3%A7%-C3%B5es%20criminosas. Sobre a ação, ver notícia do site do STF, disponível em https://portal.stf.jus.br/processos/detalhe.asp?incidente=4483504. Acesso em: 31.07.2015.

38. Francisco Brito Cruz, diretor do InternetLab, informa que "no Brasil, o Núcleo de Informação e Coordenação do Ponto BR (NIC.br), braço operativo do Comitê Gestor da Internet, é o responsável por criar as regras sobre como provedores de conexão podem inscrever-se como "sistemas autônomos", participando assim da distribuição de blocos de números IP feita pelo NIC.br. Segundo o NIC.br, as entidades precisam possuir, por exemplo, "uma mínima infraestrutura de rede" e "ter 2 ou mais conexões independentes à Internet ou então uma conexão com uma operadora e uma conexão a um ponto de troca de tráfego", além de uma série de padrões técnicos e equipe compatível. Fontes: ‹http://registro.br/tecnologia/provedor-acesso.html?secao=numeracao› e ‹ftp://ftp.registro.br/pub/gter/gter28/07-Asbr.pdf ›." Diante disso, nem todo provedor de conexão à Internet preenche a definição do Marco Civil da Internet que instituição a obrigação da guarda de registros de conexão.

39. TRIBUNAL DE JUSTIÇA DE SÃO PAULO. Agravo de Instrumento nº 2150710-76.2015.8.26.0000. Agravante: Google Brasil Internet Ltda.; Agravada: Tim Celular S.A. Rel. Des. Alexandre Marcondes, julg. 31.08.2015, entendendo que informação sobre portas lógica utilizada no acesso à internet é própria de provedor de conexão.

40. TRIBUNAL DE JUSTIÇA DE SÃO PAULO. Agravo de Instrumento 2206954-25.2015.8.26.0000. Agravante: Google Brasil Internet Ltda.; Agravado: Itaú Unibanco S.A. Relator Desembargador Paulo Alcides, julg. 12.05.2016, determinando que provedor de aplicação informe a porta lógica de origem.

41. Sobre a discussão, ver BRITO CRUZ, Francisco, Comentário a "Porta Lógica e provedores de aplicação", *Observatório do Marco Civil da Internet*, 01 de junho de 2016, disponível em: http://www.omci.org.br/jurisprudencia/99/porta-logica-e-provedores-de-aplicacao/. Acesso em 17.01.2016 (contra a determinação de fornecimento de porta lógica); OPICE BLUM, Renato, "Portas Lógicas de Origem: identificação e caos jurídico", *Jota*, 26.10.2016. Disponível em: http://jota.info/artigos/direito-digital-portas-logicas-de-origem-dificuldade-de-identificacao-e-o-caos-juridico-26102016. Acesso em: 17.01.2016 (a favor da existência de obrigação de fornecimento de tais dados); LOPES, Marcelo Frullani. Entrave tecnológico provoca impasse sobre o Marco Civil e anonimato, Consultor Jurídico, 17.12.2016. Disponível em: https://www.conjur.com.br/2016-dez-17/entrave-tecnologico-provoca-impasse-marco-civil-anonimato#:~:text=Entrave%20tecnol%C3%B-3gico%20provoca%20impasse%20sobre%20Marco%20Civil%20e%20anonimato,-17%20de%20dezembro&text=A%20veda%C3%A7%C3%A30%20

ao%20anonimato%20prevista,desde%20a%20dissemina%C3%A7%C3%A3o%20da%20internet. Acesso em: 17.01.2016 (defendendo que provedor de conexão pode ser responsabilizado caso não seja possível identificar usuário quando utilizado o protocolo NAT).

42. No sentido da necessidade da retenção da porta lógica, ver: STJ - REsp: 1777769 SP 2018/0292747-0, Relator: Ministra NANCY ANDRIGHI, Data de Julgamento: 05/11/2019, T3 - TERCEIRA TURMA, Data de Publicação: DJe 08/11/2019. "PROCESSUAL CIVIL. RECURSO ESPECIAL. AÇÃO DE OBRIGAÇÃO DE FAZER. INTERNET. PROVEDOR DE APLICAÇÃO. USUÁRIOS. IDENTIFICAÇÃO. ENDEREÇO IP. PORTA LÓGICA DE ORIGEM. DEVER. GUARDA DOS DADOS. OBRIGAÇÃO. MARCO CIVIL DA INTERNET. INTERPRETAÇÃO TELEOLÓGICA. [...] 9. Apenas com a porta lógica de origem é possível fazer restabelecer a univocidade dos números IP na internet e, assim, é dado essencial para o correto funcionamento da rede e de seus agentes operando sobre ela. Portanto, sua guarda é fundamental para a preservação de possíveis interesses legítimos a serem protegidos em lides judiciais ou em investigações criminais. 10. Recurso especial não provido."

43. No sentido da interpretação literal do Marco Civil da Internet, ver: TJ-RS - AI: 70079761847 RS, Relator: Eugênio Facchini Neto, Data de Julgamento: 27/02/2019, Nona Câmara Cível, Data de Publicação: Diário da Justiça do dia 01/03/2019. "AGRAVO DE INSTRUMENTO. RESPONSABILIDADE CIVIL. AÇÃO INDENIZATÓRIA C/C OBRIGAÇÃO DE FAZER. DETERMINAÇÃO DE FORNECIMENTO DE PORTA LÓGICA DE ENDEREÇO DE USUÁRIO. AUSENTE PREVISÃO LEGAL. Nos termos dos artigos 5º e 15 da Lei nº 12.965/2014 (Marco Civl da Internet) não há previsão legal para que os provedores de aplicação à Internet (Facebook) forneçam a porta lógica relativa ao IP de usuário, mas tão somente armazenem o endereço do IP, data e hora de acesso. Ademais, no caso, não há periculum in mora no presente caso, visto que o agravante já forneceu o nome, endereço e telefone celular do usuário, bem como o perfil já foi bloqueado. AGRAVO DE INSTRUMENTO PROVIDO.

44. Ver BRITO CRUZ, Francisco, et. al., "O que está em jogo na regulamentação do Marco Civil?, InternetLab, 2015, p. 32. Disponível em https://internetlab.org.br/pt/noticias/o-que-esta-em-jogo-na-regulamentacao-do-marco-civil-da-internet/. Acesso em 13.09.2015.

45. Ver manifestações nesse sentido em https://internetlab.org.br/pt/internetlab-reporta/internetlab-reporta-consultas-publicas-no-04/,http://www.internetlab.org.br/pt/internetlab-reporta/internetlab-reporta-consultas-publicas-no-04/.

46. Ver: Ferraz Júnior, T. S. (2018). Sigilo de dados, o direito à privacidade e os limites do poder do Estado: 25 anos depois. In: Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate. Vol. I. São Paulo: InternetLab,

pp. 18-41; e Ferraz Júnior, T. S. (2021). O alcance da proteção do sigilo das comunicações no Brasil. In: Direitos fundamentais e processo penal na era digital: Doutrina e Prática em Debate. Vol. IV. São Paulo: InternetLab, 2021.

47. Críticas elaboradas pelos pesquisadores Riana Pfefferkorn, Carlos Fico, Jacqueline Abreu, Amber Sinha e Glenn Greenwald, entrevistados pelo InternetLab na elaboração do relatório "Rastrear o viral? Riscos à privacidade no projeto de lei 'de combate às fake news'", disponível em: https://bit.ly/3PHOK9h

48. Fazendo o mesmo diagnóstico, MENDES, Gilmar Ferreira; PINHEIRO, Jurandi Borges. "Interceptações e privacidade: novas tecnologias e a Constituição". In: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P.(coord.). *Direito, Inovação e Tecnologia*. Volume 1. São Paulo: Saraiva, 2015, pp. 231-250, p. 237.

49. SUPERIOR TRIBUNAL DE JUSTIÇA. Habeas Corpus nº 315.220-RS, Min. rel. Maria Thereza de Assis Moura, julg. 15.09.2015 (considerando que a quebra de correio eletrônico só pode ser decretada diante de requisites próprios de cautelaridade que a justifiquem, devendo a providência ser imprescindível e o lapso temporal bem delineado segundo o princípio da proporcionalidade).

50. Neste sentido, ver também AZEREDO, João Fábio A. "Sigilo das Comunicações Eletrônicas diante do Marco Civil da Internet" in: DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de (coord.). *Direito & Internet III*. Tomo II. São Paulo: Quartier Latin, pp. 211-31, 2015, p. 227.

51. TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL. Agravo de Instrumento n. 70018 683508, Desembargadora Maria Berenice Dias. Julgamento: 28.07.07. Disponível em: http://jus.com.br/jurisprudencia/16757/tjrs-autoriza-interceptacao-telefonica-para-localizar-devedor-de-alimentos. Acesso em: 17.06.2015.

52. JUSTIÇA FEDERAL. Seção Judiciária de São Paulo. Mandado de Segurança n. 0001972-91.2015.4.03.6100. Juiz Federal Djalma Moreira Gomes. Data de Julgamento: 24.04.2015. Disponível em: http://www.omci.org.br/jurisprudencia/35/vedacao-a-obtencao-de-dados-sem-ordem-judicial/.

53. São eles sequestro e cárcere privado (art. 148, Código Penal[CP]), redução à condição de escravo (art. 149, CP), tráfico de pessoas (art. 149-A, CP), extorsão mediante restrição de liberdade da vítima (art. 15, § 3º CP), extorsão mediante sequestro (art. 159, CP) e tráfico internacional de criança ou adolescente (art. 239, Estatuto da Criança e do Adolescente).

54. MACEDO, Fausto; COUTINHO, Mateus, "Operadoras de celular vão ao Supremo contra lei que obriga repasse de dados a delegados e promotores", *O Estado de*

São Paulo, 25 de janeiro de 2017, disponível em: http://politica.estadao.com.br/blogs/fausto-macedo/operadoras-de-celular-vao-ao-supremo-contra-lei-que-obriga-repasse-de-dados-a-delegados-e-promotores/. Acesso em: 31.01.2017.

55. Este argumento é elaborado, por exemplo, em BARRETO, Alesandro Gonçalves; WENDT, Emerson. "Marco Civil da Internet e Acordos de Cooperação Internacional: análise da prevalência pela aplicação da legislação nacional aos provedores de conteúdo internacionais com usuários no Brasil", *Direito & TI*, 30 de agosto de 2015, disponível em: https://direitoeti.com.br/direitoeti/article/view/3

56. Segundo o relator do projeto, Deputado Alessandro Molon, "as modificações foram promovidas tendo em vista que hojá há questionamentos em relação a qual é a jurisdição aplicável quando os dados de brasileiros estão localizados no exterior. Não é incomum se ouvir que não se aplica a lei brasileira à nossa proteção quando nossos dados estão localizados no exterior. Para dirimir dúvidas, acolhendo sugestão do Governo, optamos por incluir este dispositivo no Marco Civil da Internet". Ver MADRUGA, Antenor; FELDENS, Luciano. Dados Eletrônicos e cooperação internacional: limites jurisdicionais in: MINISTÉRIO PÚBLICO FEDERAL, Temas de Cooperação Internacional, 2ª Edição revista e ampliada, vol. 2, Brasília: MPF, pp. 49-70, 2016, p. 64; BRITO CRUZ, Francisco de Carvalho. Direito, Democracia e Cultura Digital: a experiência de elaboração legislativa do Marco Civil da Internet. Dissertação de Mestrado apresentada à Faculdade de Direito da Universidade de São Paulo, 2015, p. 114.

57. Ver ABREU, Jacqueline de Souza, "From Jurisdictional Battles to Crypto Wars: Brazilian Courts v. WhatsApp", *Columbia Journal of Transnational Law Online Edition*, 17 de outubro de 2016, disponível em http://jtl.columbia.edu/from-jurisdictional-battles-to-crypto-wars-brazilian-courts-v-whatsapp/. Acesso em: 20.01.2017.

58. Ver ACCIOLY, Hildebrando; SILVA, G. E. do Nascimento; CASELLA, Paulo Borba. *Manual de Direito Internacional Público*. 18ª Edição. São Paulo: Saraiva, 2010, p. 321.

59. SOUZA, Carolina Yumi de. "Cooperação jurídica internacional em matéria penal: considerações práticas", *RBCCRIM*, vol. 71, pp. 297-325, 2008, p. 300.

60. Um exemplo disso é o acordo entre a Polícia Federal e a empresa canadense "Research in Motion", fabricante do celular Blackberry. Segundo notícias, no âmbito da Lava Jato, mensagens do doleiro Alberto Youssef, só foram acessadas "porque [a PF] conseguiu convencer a BlackBerry a franquear acesso às conversas feitas por BBM, serviço de mensagens instantâneas dos aparelhos da marca". Ver BORBA, Julia; NERY, Natuza, "PF quer instalar vírus em telefone grampeado para copiar informações", *Folha De São Paulo*, 27 de abril de 2015, disponível em: https://www1.folha.uol.com.br/poder/2015/04/1621459-pf-quer-instalar-virus-em-telefone-grampeado-para-copiar-informacoes.shtml. Acesso em 03.02.2017. Esse "canal direto"

"dribla" acordos internacionais de cooperação mútua, já que sequer passam pelo Ministério da Justiça. Ver mais sobre a controvérsia em CANÁRIO, Pedro, "Relação direta entre PF e empresa canadense alarma advogados da 'lava jato'", *Consultor Jurídico*, 10 de novembro de 2015, disponível em: http://www.conjur.com.br/2015-nov-10/relacao-entre-pf-empresa-canadense-alarma-advogados-lava-jato. Acesso em: 03.02.2017.

61. Para uma análise mais detalhada do assunto, ver: ELETRONIC FRONTIER FOUNDATION, Joint Civil Society Response to Discussion Guide on a 2nd Additional Protocol to the Budapest Convention on Cybercrime. Disponível em: https://www.eff.org/pt-br/document/joint-civil-society-response-discussion-guide-2nd-additional-protocol-budapest-convention. Acesso em: 26 de julho de 2022.

62. SUPERIOR TRIBUNAL DE JUSTIÇA, Recurso em Mandado de Segurança nº 46.685/MT. Min. rel. Leopoldo de Arruda Raposo, julg. 26.03.2015.

63. SCOCUGLIA, Livia. "MPF deve obter dados do Facebook nos EUA por tratado", Jota, 02 de dezembro de 2016, disponível em: https://www.jota.info/justica/mpf-deve-obter-por-tratado-dados-de-rede-social-diz-juiz-02122016. Acesso em: 19.01.2017.

64. O processo nº 0013254-29.2015.4.03.6100 relativo à Ação Civil Pública proposta pelo MPF contra a Facebook Brasil pode ser acompanhado na plataforma Observatório do Marco Civil, em http://www.omci.org.br/jurisprudencia/117/descumprimento-de-ordem-de-autoridade/. A decisão mais recente do Tribunal Regional Federal da 3ª Região é de 20 de julho de 2016. Em 26 de janeiro de 2017, foi admitido recurso especial do MPF ao STJ.

65. SUPERIOR TRIBUNAL DE JUSTIÇA, Recurso em Mandado de Segurança nº 55.109/PR. Min. rel. Reynaldo Soares da Fonseca, julg. 07.11.2017

66. SUPERIOR TRIBUNAL DE JUSTIÇA, Recurso em Mandado de Segurança nº 55.019/DF. Min. rel. Joel Ilan Parciornik, julg. 12.12.2017

67. VIDE o acórdão do RMS nº RMS 55.109/PR, já referenciado.

68. SUPREMO TRIBUNAL FEDERAL. Ação Declaratória de Constitucionalidade nº 51. Min. rel. Gilmar Mendes, instaurado em 28.11.2017.

69. As informações estão disponíveis em https://transparencyreport.google.com/?hl=pt_BR,https://www.microsoft.com/about/csr/transparencyhub/lerr/, https://privacy.microsoft.com/en-us/privacy-report. Acesso em: 06.07.2022.

70. SUPREMO TRIBUNAL FEDERAL. Ação Direta de Inconstitucionalidade n. 1488-9/DF, Min. Néri da Silveira, julg. em 07.11.1999.

71. Ver, do SUPREMO TRIBUNAL FEDERAL, por exemplo, o Habeas Corpus 84.301-SP, Min. rel. Joaquim Barbosa, julg. em 09.11.2004 (disponível em, https://portal.stf.jus.br/processos/detalhe.asp?incidente=2220924; acesso em 03.08.15) e o Habeas Corpus 83.515-RS, Min. rel. Nelson Jobim, julg. em 16.09.2005 (disponível em https://portal.stf.jus.br/processos/detalhe.asp?incidente=2166467; acesso em 03.08.15).

72. SUPREMO TRIBUNAL FEDERAL. Recurso Extraordinário nº 625263. Min. rel. Gilmar Mendes, julg. em 17.03.2022.

73. Tese fixada pelo RE supracitado, cristalizada como "Tema 661" do STF.

74. CORTE INTERAMERICANA DE DIREITOS HUMANOS. Caso Escher e outros vs. Brasil. Sentença de 06.07.09. Disponível em https://www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf. Acesso em: 17.06.2015. Ver também MASI, Carlos Velho. O caso Escher e outros v. Brasil e o sigilo das comunicações telefônicas. *Revista dos Tribunais*, v. 932, Junho de 2013, pp. 309-52.

75. Ver https://bit.ly/3BCZC41. Acesso em: 11 de julho de 2022.

76. Ver estatísticas disponíveis em https://www.uscourts.gov/statistics-reports/wiretap-report-2021. Acesso em 19.07.2022.

77. TELEFÓNICA, Informe de Transparencia en las Comunicaciones 2016, Brasil, p. 11, disponível em: https://www.telefonica.com/documents/364672/127737347/Telefonica_Transparencia_ESP_interactivo_22B.pdf/e39832d1-0622-4d1b-bbfd-510af449de86. Acesso em: 06.05.2017. A empresa esclarece no início do relatório que considera "interceptações de comunicações" tanto pedidos de interceptação em tempo real de *conteúdo* quanto de interceptação em tempo real de dados de tráfego. Na parte do Brasil, cita a Lei de Interceptações como referência normativa ao falar de interceptações, além de resoluções da ANATEL e da própria Constituição Federal.

78. A aparente discrepância não parece ser um problema só no Brasil. Também parece haver desencontros entre as estatísticas oficiais divulgadas pelo Ministério da Justiça alemão (https://bit.ly/3cVqim6) e os "requerimentos" de interceptações apontados pela Telefónica para a Alemanha em seu relatório de transparência. Nos Estados Unidos também já se apontou a discrepância entre as estatísticas divulgadas por empresas e as divulgadas pelo governo. Ver GIDARI, Albert, "Wiretap Report not so Transparent", *The Center for Internet & Society at Stanford Law School Blog*, 27 de janeiro de 2017, disponível em https://cyberlaw.stanford.edu/blog/2017/01/wiretap-reports-not-so-transparent. Acesso em: 06.05.2017. As estatísticas oficiais de autoridades são sempre menores que as apontadas pelas empresas.

79. Ver, como exemplo, a seguinte entrevista com o criminalista Leonardo Sica: GRILLO, Brenno, "Quebrar sigilo de comunicação em investigações virou fetiche de autoridades", *Consultor Jurídico*, 29 de janeiro de 2017, disponível em: https://bit.ly/3vHUqlh. Acesso em: 31.01.2017.

80. Atualmente, essa contratação também é alvo de controvérsias: O TCU suspendeu o pregão eletrônico que contratou o sistema "substituto" da Harpia Tech, Ver. MOTORYN, Paulo. TCU não liberou compra do Pegasus pelo governo, mas perigo da Harpia é similar; entenda o caso. *Brasil de Fato*. Brasília, DF. Disponível em: https://bit.ly/3vFzcuw. Acesso em: 18 de julho de 2022.

81. Além do Pegasus, Carlos Bolsonaro queria outra ferramenta para espionagem dentro do governo. *ISTOÉ*. 03 de agosto de 2021. Disponível em:https://istoe.com.br/alem-do-pegasus-carlos-bolsonaro-queria-outra-ferramenta-para-espionagem-dentro-do-governo/. Acesso em: 18 de julho de 2022.

82. Sobre o tema, ver MENDES, Laura Schertel, "Uso de softwares espiões pela polícia: prática legal?", *Jota*, publicada em 04 de junho de 2015, disponível em https://bit.ly/3Sqwt1V. Acesso: 03.08.15. Mendes ressalta que a infecção de dispositivos eletrônicos por cavalos de troia é capaz de levantar todas as informações armazenadas no aparelho. Isso vai além da interceptação do *fluxo* da comunicação, restrição regulamentada pela Lei de Interceptações Telefônicas. Ressalta também que, na Alemanha, a análise da constitucionalidade deste tipo de procedimento levou o Tribunal Constitucional Federal alemão a concluir pela existência de um direito fundamental à confiabilidade e integridade de sistemas informáticos. Ver também MENDES, Gilmar Ferreira; PINHEIRO, Jurandi Borges. "Interceptações e privacidade: novas tecnologias e a Constituição". In: MENDES, Gilmar Ferreira; SARLET, Ingo Wolfgang; COELHO, Alexandre Zavaglia P. (coord.). *Direito, Inovação e Tecnologia*. Volume 1. São Paulo: Saraiva, 2015, pp. 231-250, p. 237-40 (argumentando que em face "da inexistência de lei específica sobre a matéria e da manifesta insuficiência das disposições da Lei n. 9.296/96, a infiltração clandestina em computadores pessoais mostra-se de difícil conformação com a garantia constitucional do direito à privacidade").

83. SUPERIOR TRIBUNAL DE JUSTIÇA. Sexta Turma. Recurso em Habeas Corpus nº 99.735/SC. Min. rel. Laurita Vaz, julg. em 27 de novembro de 2018.

84. Notícias ilustram esse tipo de compartilhamento. Ver VALENTE, Rubens; BRAGON, Ranier, "Abin espionou indígenas e ONGs no governo Dilma", *Folha de São Paulo*, 09 de maio de 2017, disponível em http://m.folha.uol.com.br/poder/2017/05/1882257-abin-espionou-indigenas-e-ongs-no-governo-dilma.shtml?cmpid=facefolha. Acesso em: 09.05.2017.

85. Esse entendimento é afirmado na jurisprudência. Ver SUPERIOR TRIBUNAL DE JUSTIÇA, HC 149250-SP, Min. Rel. Adilson Vieria Macabul julg. 16.05.12, que considerou interceptações realizadas com participações de agentes da ABIN no âmbito da Operação Satiagraha ilegais. É também o manifestado publicamente pela ABIN. Em resposta à pergunta "A ABIN faz escuta telefônica?" em seu site, o que se lê é "Não. A Lei 9.296, de 24 de julho de 1996, que regulamenta o dispositivo constitucional, art. 5º, inciso XII, estabelece os órgãos competentes para executar, com autorização judicial, a interceptação telefônica. A ABIN não se enquadra nessa determinação legal." Disponível em: https://www.gov.br/abin/pt-br/acesso-a-informacao/perguntas-frequentes/a-abin (Acesso em: 07.07.2022). A agência já foi, entretanto, acusada publicamente de realizar interceptações do Ministro do Supremo Tribunal Federal Gilmar Mendes, em escândalo revelado em 2008. Ver FOLHA DE SÃO PAULO, "Divulgação de grampo a presidente do STF derruba diretoria da Abin", 07 de novembro de 2008, disponível em http://www1.folha.uol.com.br/fsp/corrida/cro709200802.htm . Acesso em: 31.07.2015.

86. FOLHA DE SÃO PAULO, "Acesso ao Guardião pela Abin gera polêmica", 12 de novembro de 2008, disponível em: http://www1.folha.uol.com.br/fsp/brasil/fc1211200805.htm. Acesso em: 17.06.2015.

87. Supremo Tribunal Federal, ADI 6529 DF, Relator: Cármen Lúcia, julg. 11.10.2021, Tribunal Pleno, p. 22.10.2021.

88. https://bit.ly/3zXYN4w

ESTE LIVRO FOI COMPOSTO COM AS FAMÍLIAS TIPOGRÁFICAS *DECIMA MONO* E *FF META*. PARA O MIOLO FOI UTILIZADO O PAPEL COUCHE FOSCO E PARA A CAPA O PAPEL DUO DESIGN. O PROJETO GRÁFICO É DE AUTORIA DO *ESTÚDIO CLARABOIA*. FORAM IMPRESSAS 250 CÓPIAS PELA *GRÁFICA CINELÂNDIA* EM 2022.