INTERNETLAB

# VIGILÂNCIA SOBRE AS COMUNICAÇÕES NO BRASIL

Interceptações, quebras de sigilo, infiltrações e seus limites constitucionais

2017

Jacqueline de Souza Abreu
Dennys Antonialli

segunda edição

INTERNETLAB

# VIGILÂNCIA SOBRE AS COMUNICAÇÕES NO BRASIL

Interceptações, quebras de sigilo, infiltrações e seus limites constitucionais

2017

Jacqueline de Souza Abreu
Dennys Antonialli

A primeira edição deste relatório, lançada em setembro de 2015, foi elaborada como parte do projeto "Vigilância e Direitos Humanos" realizado em oito países da América Latina em parceria com a Electronic Frontier Foundation, uma organização internacional sem fins lucrativos que, desde 1990, defende a liberdade de expressão e a privacidade na era digital. A continuação deste projeto e a revisão e atualização do relatório é de responsabilidade apenas do INTERNETLAB. Esta edição foi fechada em 08 de maio de 2017.

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:**
ABREU, Jacqueline de Souza; ANTONIALLI, Dennys.
*Vigilância sobre as comunicações no Brasil: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais.*
São Paulo: InternetLab, 2017.



## AUTORES

**JACQUELINE DE SOUZA ABREU**

Doutoranda em filosofia e teoria geral do direito na Universidade de São Paulo e pesquisadora no INTERNETLAB. É mestra em Direito, com especialização em Direito e Tecnologia, pela Universidade de California, Berkeley (LL.M., 2016) e também, com especialização em Direito Constitucional, pela Universidade Ludwig Maximilian de Munique (LL.M., 2015). É bacharela em Direito pela Universidade de São Paulo (LL.B., 2014). Durante seus estudos, recebeu bolsas de estudo da Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) e do Serviço Alemão de Intercâmbio Acadêmico (DAAD). Foi membro do Núcleo de Direito, Internet e Sociedade da Faculdade de Direito da USP e assistente de pesquisa no Berkman Center for Internet & Society na Universidade Harvard.

**DENNYS ANTONIALLI**

Doutor em direito constitucional pela Universidade de São Paulo, com graduação em direito pela mesma universidade (2008), mestrado em direito pela Universidade de Stanford (JSM, 2011) e mestrado profissional em "Law and Business", conjuntamente oferecido pela Bucerius Law School e pela WHU Otto Beisheim School of Management (MLB, 2010). Atuou junto à equipe de políticas públicas em tecnologia e direitos civis na American Civil Liberties Union of Northern California (ACLU/NC) e como consultor jurídico do "Timor Leste Legal Education Project", da Stanford Law School/Asia Foundation. Foi ganhador do 1º lugar do Steven M. Block Civil Liberties Award da Stanford Law School (2011) e do 1º lugar do Prêmio Marco Civil da Internet e Desenvolvimento da Escola de Direito da Fundação Getúlio Vargas (SP). Foi pesquisador do Alexander von Humboldt Institute for Internet and Society (Berlim) e participou do Summer Doctoral Program do Oxford Internet Institute. Advogado, atualmente é coordenador do Núcleo de Direito, Internet e Sociedade da FDUSP (NDIS) e diretor do INTERNETLAB.

## COLABORARAM

PAULA PÉCORA DE BARROS
INTERNETLAB

BEATRIZ KIRA
INTERNETLAB

# APRESENTAÇÃO

O objetivo deste relatório é oferecer um panorama sobre o quadro normativo referente às capacidaades e prerrogativas de vigilância das comunicações por autoridades estatais no Brasil. Além dos direitos e garantias previstos na Constituição Federal e dos dispositivos previstos na legislação, são analisados casos, notícias e decisões judiciais que ilustram as principais questões controversas no que diz respeito a práticas de vigilância por parte das autoridades estatais no país. Para delimitar o escopo deste estudo, trabalhou-se com a seguinte definição de *vigilância das comunicações*: quaisquer atividades que envolvam interceptações, monitoramento, análise, uso, guarda e obtenção de informações que incluam ou reflitam comunicações passadas, presentes ou futuras de alguma pessoa ou que surjam a partir delas.

Em 2015, o INTERNETLAB, em parceria com a Electronic Frontier Foundation, lançou relatório com mesmo objetivo e escopo. Esta pesquisa constitui uma versão[1] expandida e atualizada daquela versão. Além de revisar o panorama normativo referente ao tema, o texto inclui seções 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)* a extraterritorialidade do Marco Civil da Internet e os conflitos judiciais daí decorrentes no que diz respeito ao acesso a dados de usuários detidos por empresas de Internet sediadas no exterior; *(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 2016. Essa e outras informações obtidas via Lei de Acesso à Informação foram incluídas em anexos ao fim deste relatório.

Em linhas gerais, o leitor pode esperar deste relatório a apresentação do estado normativo da vigilância do Estado sobre as comunicações no Brasil em 2017. 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].

**[NOTA 1]** ABREU, Jacqueline de Souza; ANTONIALLI, Dennys. *"Vigilância das comunicações pelo 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.

**[NOTA 2]** Ver https://pt.necessaryandproportionate.org/text.

# 1
# PANORAMA NORMATIVO

O quadro 1 apresenta um panorama geral sobre as normas constitucionais e legais gerais que impõem limites à vigilância sobre as comunicações no Brasil. O quadro 2 indica as instituições estatais associadas a práticas de vigilância e explica suas funções. O quadro 3 resume a abrangência da vigilância estatal brasileira sobre as comunicações, apresentando informações que serão detalhadas ao longo deste relatório. O quadro 4 aponta para a extensão que determinadas práticas de vigilância envolvendo o Estado brasileiro podem assumir em decorrência de acordos e arranjos de cooperação judiciária internacional em matéria penal.

## QUADRO 1
## LIMITES GERAIS À VIGILÂNCIA SOBRE AS COMUNICAÇÕES NO BRASIL

| | |
|---|---|
| **DIREITOS** | Constituição Federal protege a liberdade de expressão, a intimidade e o sigilo das comunicações (art. 5º incisos IX, X e XII).<br><br>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.<br><br>Não há testes consagrados, de aplicação uniformizada na jurisprudência e na doutrina, para avaliação da constitucionalidade de restrições a esses direitos.<br><br>O art. 5º, § 2º da Constituição Federal dispõe que direitos e garantias expressos nela 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).<br><br>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. 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.<br><br>Art. 156-A do Código Penal criminaliza invasão a dispositivo informático com 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. |

Autoria própria

## 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).<br><br>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. |
| **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. Controle externo da atuação é exercido pelo Ministério Público (art. 129, VII, CF).<br><br>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). 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).<br><br>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** | Nos termos da Lei nº 9.833/99, compete à ABIN, órgão central do Sistema Brasileiro de Inteligência (SISBIN), planejar, executar, supervisionar e controlar as atividades de inteligência. Pelo Decreto nº 4.376/02, compõem também o Sisbin a Casa Civil e o Gabinete de Segurança Institucional da Presidência da República e diversos Ministérios e órgãos a eles relacionados (como Polícia Federal, pelo Ministério da Justiça, e Receita Federal, pelo Ministério da Fazenda). Controle externo é exercido por Comissão Mista permanente no Congresso Nacional, em obediência ao art. 6º da Lei nº 9833/99.<br><br>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). Não há impedimentos para monitoramento de comunicações públicas. |

Autoria própria

## QUADRO 3
## VIGILÂNCIA DO ESTADO BRASILEIRO SOBRE AS COMUNICAÇÕES

| FIM / AUTORIDADE(S) | REGULAÇÃO DAS TELECOMUNICAÇÕES (ANATEL) | *LAW ENFORCEMENT* (AUTORIDADES POLICIAIS, MINISTÉRIO PÚBLICO, JUÍZES E CPIs) | INTELIGÊNCIA (SISBIN) |
|---|---|---|---|
| **OBRIGAÇÕES DE GUARDA DE DADOS** | Resoluções nº 426/05, 477/07 e 614/13 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. | 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.<br><br>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. | Não há obrigação de guarda expressamente para fins de inteligência. |

| FIM / AUTORIDADE(S) | REGULAÇÃO DAS TELECOMUNICAÇÕES (ANATEL) | *LAW ENFORCEMENT* (AUTORIDADES POLICIAIS, MINISTÉRIO PÚBLICO, JUÍZES E CPIS) | INTELIGÊNCIA (SISBIN) |
|---|---|---|---|
| **ACESSO A DADOS ARMAZENADOS (INFORMAÇÕES CADASTRAIS E METADADOS)** | No exercício de poderes fiscalizatórios (art. 8º, Lei 9472/97), a ANATEL pode acessar documentos fiscais, que contêm informações cadastrais e registros, por requisição às prestadoras de serviço. Atualmente, há desenvolvimento de infraestrutura que permita acesso direto e irrestrito online, baseada no art. 38 da Resolução nº 596/12.<br><br>Receita Federal também pode exigir acesso aos documentos fiscais (art. 11, Lei nº 8.218/91). | 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, 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.<br>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.<br>Pelo MS 23452/RJ do STF, acesso a registros telefônicos também pode ocorrer no âmbito de CPIs.<br><br>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). | 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. |

| FIM / AUTORIDADE(S) | REGULAÇÃO DAS TELECOMUNICAÇÕES (ANATEL) | *LAW ENFORCEMENT* (AUTORIDADES POLICIAIS, MINISTÉRIO PÚBLICO, JUÍZES E CPIs) | INTELIGÊNCIA (SISBIN) |
|---|---|---|---|
| **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. | 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. | 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. | 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. | 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). |

Autoria própria

## QUADRO 4
## COOPERAÇÃO JURÍDICA 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 em 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 |

Autoria própria.

Fonte das informações: BELOTTO, Ana Maria de Souza; MADRUGA, Antenor; TOSI, Mariana Tumbiolo, *Dupla incriminação na cooperação jurídica internacional*, in: Boletim IBCCRIM, n. 237, Agosto 2012, disponível em: http://www.ibccrim.org.br/boletim_artigo/4678-Dupla-incriminao-na-cooperao-jurdica-internacional Acesso: 31.07.2015.

# 2 ANÁLISE: VIRTUDES E PROBLEMAS

## 2.1. FRAGILIDADES DE NÍVEL *CONSTITUCIONAL* NA PROTEÇÃO CONTRA VIGILÂNCIA INDEVIDA

A Constituição Federal brasileira de 1988 contém, no rol dos direitos fundamentais, ao menos três 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"). Apesar de a Constituição proteger o sigilo das comunicações e a privacidade, disputas interpretativas 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 abusiva 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 até hoje predominante[3], que também encontra eco em decisão do Supremo Tribunal Federal[4], é no sentido de que *(i)* a proteção

**[NOTA 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.

**[NOTA 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.

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, portanto, 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.[5] 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 fun-

**[nota 5]** 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; 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; 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, pp. 222-3; ANTONIALLI, Dennys; BRITO CRUZ, Francisco; VALENTE, Mariana G., "*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/. Em termos de jurisprudência internacional, na decisão do caso Escher na Corte Interamericana de Direitos Humanos, que inclusive resultou em condenação ao Brasil (caso analisado neste relatório mais à frente), a CIDH também reconheceu expressamente que o direito à privacidade abarca não só a proteção do conteúdo das comunicações, como também dos metadados. Ver CORTE INTERAMERICANA DE DIREITOS HUMANOS. Caso Escher e outros vs. Brasil. Sentença de 06.07.09, Parágrafo 114. Disponível em http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf Acesso em: 08.05.2017.

**[nota 6]** No habeas corpus 70814/SP (Min. Rel. Celso de Mello, julg. em 01.03.2004), por exemplo, o Supremo Tribunal Federal admitiu que a administração penitenciária pode interceptar carta de preso, por razões de segurança pública, disciplina prisional ou preservação da ordem jurídica, com base no art. 41, parágrafo único, da Lei 7210/84, a lei de Execuções Penais, que restringe o direito do preso "ao contato com o mundo exterior por meio de correspondência escrita" (art. 41, XV, da mesma lei). Sobre isso, ver também MENDES, Gilmar; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. *Curso de Direito Constitucional*. 2ª ed. rev. e atual. São Paulo: Saraiva, 2008, p. 392; MORAIS, Alexandre. *Direito Constitucional*. 28ª Ed. São Paulo: Atlas, 2012, p. 59. Mais questões que contestam a validade da interpretação restrita dada ao inciso XII do art. 5º são apresentadas ao longo do relatório.

damental conflitante ou em interesse público.[6] 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").[7] Em 2014, o Congresso também voltou a explicitamente admitir interceptações de comunicações eletrônicas (que, igualmente, envolvem "dados") no Marco Civil da Internet.

## GRADAÇÕES DE PRIVACIDADE: INFORMAÇÕES CADASTRAIS < METADADOS < CONTEÚDO?

Mesmo que apenas o *fluxo* das comunicações seja tido como 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[8], 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 relatório, 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 relatório, consideram-se metadados todos os dados e registros gerados a partir de uma comunicação e que não constituam o seu conteúdo em si, como, por exemplo, data, hora e duração da comunicação, remetente, destinatários, eventuais dados de localização geográfica do dispositivo (como Estação Rádio Base), códigos de identificação de dispositivos (como IMEI), etc.

### CONTEÚDO DAS COMUNICAÇÕES

Para fins deste relatório, considera-se conteúdo das comunicações todas as informações que dizem respeito à dimensão da mensagem da comunicação entre dois ou mais indivíduos (o emissor e seus receptores), 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 relatório, 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.

**[NOTA 7]** Trata-se da Lei Federal nº 9.296/96, a qual se discutirá posteriormente.

**[NOTA 8]** 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 http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=605418. 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.

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 recentes que têm facilitado a obtenção dessas informações por mera requisição de autoridades, retirando a necessidade de ordem judicial.[9] 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 têm surgido, 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 fieis 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

**[NOTA 9]** Alterações legislativas recentes "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.

grampos ou escutas ambientais. Para tanto, estabeleceu um regime jurídico rigoroso, que envolve o preenchimento de requisitos mais difíceis de ser atendidos em razão da grandeza da intrusão que 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.[10] Na doutrina[11], também já começa a se argumentar 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 setembro de 2016, já afastou essa tese. Na mesma decisão, afirmou a legalidade da prova obtida por celulares apreendidos no âmbito da Operação Lava Jato mediante mandado de busca e apreensão, mesmo sem autorização judicial específica que delimitasse a "busca virtual".[12] 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 dez anos, as duas decisões demonstram quão penetrantes são as raízes do entendimento de que dados armazenados não estão protegidos pelo direito ao sigilo das

**[nota 10]** 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.

**[nota 11]** 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.

comunicações na jurisprudência nacional, o qual alimenta o descompasso normativo entre a proteção de comunicações em fluxo e comunicações armazenadas.

### 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 também 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 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, 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".[13] 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.[14] Em 2016, por outro lado, agora lidando com um *smartphone* e demonstrando-se ciente da enorme quantidade de dados que um celular moderno produz e armazena, o STJ decidiu que a verificação de histórico de conversas do WhatsApp (conteúdo) em celular apreendido após flagrante constitui quebra de sigilo, isto é, é ilegal sem a existência de ordem judicial autorizadora.[15]

Em tribunais estaduais, a apreciação do tema permanece casuística. Nos Tribunais de Justiça do Paraná[16], do Rio de Janeiro[17] e do Espírito Santo[18], foram encontrados julgados de 2016 que consideram que o acesso a dados de celular apreendido após flagrante prescinde de autorização judicial. A fundamentação utilizada é o

**[nota 12]** 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.

**[nota 13]** SUPREMO TRIBUNAL FEDERAL. Habeas Corpus nº 91.867/SP. Min. rel. Gilmar Mendes, julg. 24.04.2012.

**[nota 14]** SUPERIOR TRIBUNAL DE JUSTIÇA. Habeas Corpus nº 66.368/PA. Min. rel. Gilson Dipp, 5ª Turma, julg. 05.06.2007.

**[nota 15]** SUPERIOR TRIBUNAL DE JUSTIÇA. Recurso Ordinário em Habeas Corpus nº 51.531/RO. Min. rel. Nefi Cordeiro. 6ª Turma, julg. 19.04.2016.

**[nota 16]** TRIBUNAL DE JUSTIÇA DO PARANÁ. Habeas Corpus nº 1547585-9/PR. Rel. Maria José de Toledo Marcondes Teixeira. 5ª Câmara Criminal, julg. 14.07.2016.

**[nota 17]** TRIBUNAL DE JUSTIÇA DO RIO DE JANEIRO. Apelação Criminal 01963693720158190001 RJ. Rel. Marcus Henrique Pinto Basílio, Primeira Câmara Criminal, julg. 17.05.2016.

**[nota 18]** TRIBUNAL DE JUSTIÇA DO ESPÍRITO SANTO. Apelação Criminal 00070812320148080030. Rel. Sérgio Luiz Teixeira Gama, 2ª Câmara Criminal, julg. 24.02.2016.

art. 6º do Código de Processo Penal, o qual autoriza autoridades policiais a apreenderem objetos que tiverem relação com o fato delituoso e colherem todas as provas que servirem para o esclarecimento do fato e suas circunstâncias.[19] No Tribunal de Justiça do Distrito Federal[20] e na Quarta Vara Federal Criminal em São Paulo há decisões em favor da necessidade de autorização judicial, tendo em vista que o acesso a dados armazenados em celulares apreendidos constitui "busca virtual" e que celulares modernos deixaram de ser apenas instrumentos de conversação de voz. Na Sétima Vara Federal Criminal em São Paulo,[21] juiz considerou que prova obtida da verificação de mensagens de WhatsApp são ilegais; por outro lado, policiais estariam autorizados a consultar os últimos registros telefônicos para descobrir "comparsas".[22]

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.[23] 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,[24] 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,[25] 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.

**[nota 19]** Na doutrina, defesa neste mesmo sentido pode ser encontrada em BARRETO, Alesandro Gonçalves; FÉRRER, Everton Ferreira de Almeida, Perícia em celular: necessidade de autorização judicial?, *Direito & TI*, 04 de junho de 2016, disponível em http://direitoeti.com.br/artigos/pericia-em-celular-necessidade-de-autorizacao-judicial/. Acesso em: 25.01.2017.

**[nota 20]** TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E TERRITÓRIOS. Apelação Criminal 20150110776509 0023326-92.2015.8.07.0001. Rel. João Timóteo de Oliveira, 2ª Turma Criminal, julg. 03.11.2016.

**[nota 21]** "Provas obtidas em celular de preso em flagrante são ilícitas", *Consultor Jurídico*, 26 de setembro de 2015, disponível em http://www.conjur.com.br/2015-set-26/provas-obtidas-celular-preso-flagrante-sao-ilicitas. Acesso em 05.05.2017.

**[nota 22]** "Policiais causam anulação de provas por vasculharem WhatsApp sem autorização", *Consultor Jurídico*, 10 de março de 2017, disponível em http://www.conjur.com.br/2017-mar-10/policiais-vasculham-whatsapp-autorizacao-invalidam-provas. Acesso em 05.05.2017.

**[nota 23]** 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.

**[nota 24]** 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: http://www.conjur.com.br/2017-fev-06/rafael-garcia-acesso-dados-celular-exige-autorizacao-judicial Acesso em: 05.05.2017.

**[nota 25]** 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: http://direitoeti.com.br/artigos/pericia-em-celular-necessidade-de-autorizacao-judicial/ Acesso em: 05.05.2017.

## ENQUANTO ISSO, NO LEGISLATIVO...

*por Beatriz Kira*

Em 20 de fevereiro de 2017,foi apresentado pelo dep. Cleber Verde (PRB/MA) o Projeto de Lei (PL) 6960/2017,[26] que propõe alterar o Marco Civil da Internet para explicitar que a inviolabilidade e o sigilo das comunicações privadas, salvo por ordem judicial, (art. 7º, III) seriam aplicáveis tanto a informações armazenadas em terminais fixos como em terminais móveis (como celulares, smartphone, *tablets* e similares). Segundo a justificativa do PL, de autoria do dep. Cleber Verde (PRB/MA), a proposta visa esclarecer o limite de poder da autoridade policial numa eventual abordagem e impedir a devassa de dados armazenados em celulares e outros dispositivos móveis.[27]

Na contramão dessa proposta, foi apresentado em 26 de abril de 2017 o PL 7498/2017,[28] de autoria do dep. André Fufuca (PP/MA), que visa alterar o art. 7º, III, do Marco Civil da Internet para possibilitar quebra da inviolabilidade e do sigilo das comunicações privadas armazenadas por autoridade policial, independentemente de ordem judicial. Na justificativa do PL, o autor argumenta que, por conta do uso crescente de aplicativos como o WhatsApp por organizações criminosas, é imprescindível que a polícia, no momento da prisão em flagrante ou até mesmo quando da busca e apreensão, possa verificar o conteúdo de mensagens sem solicitar autorização do judiciário.[29]

### III *Utilização de criptografia de ponta-a-ponta*

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 impossibilita 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 nenhum tipo de conteúdo de conversa com a empresa no âmbito de investigações. Tal obstáculo técnico esteve por trás de decisões de bloqueio contra o aplicativo.[30] 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

**[nota 26]** Ficha de tramitação do Projeto de Lei 6960/2017 disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2124030>. Acesso em 05.05.2017.

**[nota 27]** Justificativa do Projeto de Lei 6960/2017, de autoria do dep. Cleber Verde (PRB/MA), disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1526689&filename=PL+6960/2017>. Acesso em 05.05.2017.

**[nota 28]** Ficha de tramitação do Projeto de Lei 7498/2017 disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2132356>. Acesso em 05.05.2017.

**[nota 29]** Justificativa do Projeto de Lei 7498/2017, de autoria do dep. André Fufuca (PP/MA), disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1550104&filename=PL+7498/2017>. Acesso em 05.05.2017.

**[nota 30]** 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. Ver também bloqueios.info.

inquérito civil pelo Ministério Público Federal em Rondonópolis/MT[31] bem como sinalizações, na opinião pública[32] e no atual governo[33], sobre a necessidade de regular o uso dessa tecnologia. O STF, na ADPF 403, que analisa a compatibilidade de bloqueios do WhatsApp com a Constituição Federal, também foi instado a se manifestar sobre o impasse.[34]

Mais uma vez, o que se discute é o alcance da proteção constitucional ao sigilo das comunicações. Se o art. 5, XII só admite quebra de sigilo de comunicações *telefônicas em fluxo*, não seriam apenas interceptações telefônicas que deveriam ser "grampeáveis"? Comunicações de dados seriam invioláveis? Em se tratando de tecnologia imprescindível para a confidencialidade de dados, a discussão não está só limitada a esses termos e envolve também necessariamente privacidade, liberdade de expressão e segurança individual, coletiva e nacional. 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 a arquitetura de seus serviços de modo a permitir interceptações. 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.[35]

## 2.2. ANATEL: VIGILÂNCIA SEM QUERER QUERENDO

No exercício de sua competência para expedição de normas infralegais (art. 19 da Lei nº 9.472/97), as 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 ilegítima do Estado.

**[NOTA 31]** "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.

**[NOTA 32]** 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.

**[NOTA 33]** "Governo elabora projeto para regular acesso a informações do WhatsApp, G1, 19 de julho de 2016, disponível em http://g1.globo.com/politica/noticia/2016/07/governo-elabora-projeto-para-regular-acesso-informacoes-do-whatsapp.html. Acesso em: 08.05.2017.

**[NOTA 34]** 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.

**[NOTA 35]** 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.

## OBRIGAÇÕES DE PRESTADORES DE SERVIÇOS DE TELECOMUNICAÇÕES

A Resolução nº 426/05 – Regulamento do Serviço Telefônico Fixo Comutado obriga, no art. 22, que "todos os dados relativos à prestação de serviços, inclusive os de bilhetagem", sejam guardados por prestadoras de serviço de telefonia fixa (tais como Vivo e NET) "por um prazo mínimo de 5 anos", sem precisar quais dados são esses, por quem e a que fins poderão ser usados. Não há normas específicas de segurança sobre a forma como devem ser guardados os dados: o art. 23 apenas estabelece que é responsabilidade de provedores zelar pelo sigilo dos dados. No art. 24, determina-se que prestadores de serviços de telefonia fixa tenham à disposição recursos tecnológicos e facilidades necessárias para a suspensão de sigilo das telecomunicações, decorrente e nos limites de ordem judicial, e que elas próprias devem arcar com os custos financeiros de tais tecnologias. Por meio desta resolução, são, portanto, criadas obrigações de retenção em massa de dados e também de assistência técnica para quebra de sigilo de comunicações.

Semelhantemente, a Resolução nº 477/07 – Regulamento sobre Serviço Móvel Pessoal determina, no art. 10, XXII, que prestadoras de telefonia móvel (tais como Vivo, Claro, Tim e Oi) manterão, pelo prazo mínimo de 5 anos,[36] "à disposição da Anatel e demais interessados, documentos de natureza fiscal, os quais englobam dados da ligações efetuadas e recebidas, data, horário de duração e valor da chamada, bem como informações cadastrais dos assinantes, em conformidade com o que prescreve o art. 11 da Lei 8.218/91 [...]", o qual obriga pessoas jurídicas a manterem documentos fiscais à disposição da Receita Federal pelo prazo decadencial previsto na legislação tributária, que é de 5 anos. Os arts. 42 e 58 estabelecem, ainda, "dados pessoais mínimos" para adesão de usuário a serviço de telefonia móvel (nome, número do documento de identidade e número do registro Ministério da Fazenda). Na prática, isso torna o cadastro de uma linha móvel dependente de um CPF, por exemplo, dificultando o uso anônimo. Ao art. 90, também está previsto que prestadoras tornem disponíveis "recursos tecnológicos e facilidades necessárias para a suspensão do sigilo das comunicações", sendo que equipamentos e programas utilizados para este fim devem integrar a própria plataforma de prestação de serviço da empresa. Em outras palavras, obrigatoriamente o sistema da prestadora deve ser capaz de vigilância.

A lógica da obrigação de guarda de dados relativos à prestação de serviço de telefonia por 5 anos e sua justificativa para fins fiscais e fiscalizatórios da ANATEL são indicadas pelos termos do citado art. 10, XXII da Resolução nº 477/07. Ambas as normas que estabelecem obrigações de guarda de dados na telefonia fixa e móvel sustentaram por longo período, contudo, 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 a estes fins, é apenas de 2013. Além disso, os termos das resoluções instituem obrigações de guarda de dados mesmo quando os tipos de

**[NOTA 36]** 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." Ver **ANEXO I**.

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.[37]

A Resolução nº 614/13 – Regulamento do Serviço de Comunicação Multimídia obriga provedores de conexão à Internet (tais como Vivo e NET) à guarda de registros de conexão e de dados cadastrais de assinantes pelo prazo mínimo de 1 ano, em seu art. 53. A definição de registros de conexão está fixada pelo art. 4º, XVII (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, entre outras que permitam identificar o terminal de acesso utilizado). O prazo menor se comparado às obrigações relativas à telefonia e a clareza na definição do que deve ser guardado pode ser atribuída ao fato de a resolução ter sido elaborada no contexto de discussão da Lei nº 12.965/14 ("Marco Civil da Internet") e da publicidade de decisões internacionais contrárias à retenção de dados, que receberam especial atenção da comunidade acadêmica e da sociedade civil.[38] Ainda assim, a definição prevista na resolução da ANATEL é mais abrangente que a do próprio Marco Civil da Internet, uma vez que também inclui a obrigação de guarda de "outras informações que permitam identificar o terminal de acesso utilizado", linguagem que não faz parte da definição de registros de conexão da lei em questão.[39] Por fim, o art. 52, parágrafo único da resolução, também determina que prestadoras tornem disponíveis "dados referentes à suspensão do sigilo de telecomunicações" a autoridades, obrigando que prestadoras de serviço de comunicação multimídia sejam capazes de realizar quebras de sigilo de dados e interceptações.

## ACESSO DIRETO A DADOS

O acesso da ANATEL a documentos fiscais de prestadoras de serviços, os quais, como visto, contêm informações cadastrais de clientes, registros e valores de chamadas, é admissível, em regra, para fins fiscalizatórios, por meio de requisição da agência ao prestador. Reportagem do jornal *Folha de São Paulo* de 2011[40] revelou as intenções da agência de possuir acesso *direto* e sistemático a tais dados por meio da construção de infraestrutura que permitisse acesso *online* irrestrito à ANATEL, com o objetivo de modernizar sua fiscalização. À época, a agência declarou que o acesso a registros de chamadas somente ocorreria com autorização de usuário que fizesse reclamação à agência[41] e que os *softwares* a serem instalados permitiriam apenas fornecimento

**[nota 37]** 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.

**[nota 38]** Paradigmaticamente, a decisão do caso C-293/12 pelo Tribunal de Justiça da União Europeia, de 08.04.2014, que invalidou a diretiva europeia sobre retenção de dados, sob a fundamentação de que restringiria desproporcionalmente os direitos ao respeito à vida privada e à proteção de dados pessoais. Informe à imprensa disponível em: http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf Acesso em 31.07.2015.

**[nota 39]** 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.

**[nota 40]** WIZIACK, Julio, "Anatel terá acesso total a dado sigiloso de telefones", *Folha de São Paulo*, 19 de janeiro de 2011, disponível em: http://www1.folha.uol.com.br/fsp/mercado/me1901201103.htm Acesso em: 08.05.2017.

**[nota 41]** WIZIACK, Julio, "Agência diz que não há quebra de sigilo, *Folha de São Paulo*, 19 de janeiro de 2011, disponível em http://www1.folha.uol.com.br/fsp/mercado/me1901201104.htm Acesso em: 17.06.2015.

de "informações em estado bruto" das prestadoras, não conectadas a dados cadastrais.[42] O art. 38 da Resolução nº 596/12 da ANATEL instituiu as obrigações às prestadoras de serviços de telefonia de fornecer dados, permitir o acesso e disponibilizar o acesso *online* a aplicativos, sistemas, recursos e facilidades tecnológicos utilizados por elas "para coleta, tratamento e apresentação de dados, informações e outros aspectos", confirmando as intenções da agência. As modulações da ANATEL acerca da necessidade de autorização do usuário para acesso e de especificação acerca dos dados cujo acesso é *direto* não encontraram especificações nessa resolução, contudo.

Provocada pelo INTERNETLAB, via Lei de Acesso à Informação, sobre esse programa de compartilhamento de informações, a ANATEL esclareceu, entre outras questões, quais as informações compartilhadas, quando e em que circunstâncias são compartilhadas e por que meio é feito o compartilhamento. As respostas oficiais podem ser consultadas no **ANEXO I**.

## 2.3. RECEITA FEDERAL: VIGILÂNCIA DAS COMUNICAÇÕES NAS ENTRELINHAS

O art. 10, XXII da Resolução nº 477/07 da ANATEL, visto acima, revelou que a lógica da obrigação de guarda de dados cadastrais e registros telefônicos por 5 anos está intimamente ligada 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, pelo 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, à qual se aplica a resolução citada, 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 os 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.[43] Considerando que a Receita Federal tem acesso a informações sobre comunicações de brasileiros, essa cooperação pode significar ampliação da vigilância a nível internacional.

**[NOTA 42]** GAZETA DO POVO, "Quebra de sigilo continua a depender de mandado judicial, diz Anatel", 21 de janeiro de 2011, disponível em: http://www.gazetadopovo.com.br/economia/quebra-de-sigilo-continua-a-depender-de-mandado-judicial-diz-anatel-da8drvp4kj7uyodcxir2ijw3y Acesso em: 17.06.2015.

**[NOTA 43]** Sobre isso, ver VARON FERRAZ, Joana., *Oficina Antivigilância*, Boletim n. 11, 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 http://www.itamaraty.gov.br/index.php?option=com_content&view=article&id=10389:atos-assinados-por-ocasiao-da-visita-da-presidenta-dilma-rousseff-aos-estados-unidos-washington-30-de-junho-de-2015&catid=42&Itemid=280&lang=pt-BR#neutrinos-port-8 Acesso em: 31.07.2015.

## 2.4. VIGILÂNCIA SEM E COM CONTRAPESOS: TELEFONIA VS. INTERNET

Leis federais recentes normatizaram capacidades de vigilância do Estado no exercício de atividades de segurança pública (*law enforcement*): a edição de nova Lei das Organizações Criminosas e a promulgação do Marco Civil da Internet. Enquanto a primeira dá lugar a graves problemas na proteção contra vigilância abusiva do Estado, marcadamente na área de telefonia, a segunda, elaborada em contexto de amplo e longo debate público, ao mesmo tempo cria e restringe a vigilância na Internet.

### 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 crimes praticados por organização criminosa. A inserção de uma obrigação tão abrangente em uma lei específica pode ter camuflado o aumento do poder de vigilância 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, não sendo 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 aguarda julgamento e da qual se falará mais a seguir.

#### *Prerrogativas de acesso a dados cadastrais*

O art. 15 da Lei das Organizações Criminosas dispõe 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[44] , e a Lei Complementar nº 75/93,

[NOTA 44] 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".

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.[45]

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.[46]

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.[47] 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 dessa Lei. Pelo já citado art. 15, "o

**[nota 45]** 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: http://stf.jusbrasil.com.br/jurisprudencia/22599582/recurso-extraordinario-re-716795-rs-stf Acesso em: 17.06.2015.

**[nota 46]** 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.

**[nota 47]** 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: http://www.conteudojuridico.com.br/artigo,o-sigilo-de-dados-cadastrais-dos-clientes-de-empresas--telefonicas,47762.html. Acesso em: 17.01.2017.

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.[48] A ação, proposta originalmente em 2013, ainda está pendente de julgamento.

## MARCO CIVIL DA INTERNET (LEI Nº 12.965/14)

### *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.[49] Objeto da guarda, os registros de conexão, são, segundo o art. 5º, inciso VI, "o conjunto de informa-

**[NOTA 48]** 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 http://www.conjur.com.br/2014-out-29/telefonicas-reclamam-quebras-sigilo-pedidas-delegados. Sobre a ação, ver notícia do site do STF, disponível em http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=254181 . Acesso em: 31.07.2015.

**[NOTA 49]** 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.

ções 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". 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[50] e de aplicação de internet[51].[52]

**[nota 50]** TRIBUNAL DE JUSTIÇA DE SÃO PAULO. Agravo de Instrumento n° 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.

**[nota 51]** 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.

**[nota 52]** 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://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: http://www.conjur.com.br/2016-dez-17/entrave-tecnologico-provoca-impasse-marco-civil-anonimato . Acesso em: 17.01.2016 (defendendo que provedor de conexão pode ser responsabilizado caso não seja possível identificar usuário quando utilizado o protocolo NAT).

### *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 endereço, 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.[53] 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.[54]

## ENQUANTO ISSO, NO LEGISLATIVO...

*por Beatriz Kira*

Em 6 de abril de 2016, o Senado Federal aprovou o Projeto de Lei do Senado (PLS) 730/2015,[55] de autoria do sen. Otto Alencar, que dispõe sobre a investigação criminal e a obtenção de meios de prova nos crimes praticados por intermédio de conexão ou uso de Internet. O texto final, aprovado em caráter terminativo pela Comissão Especial do Desenvolvimento Nacional (CEDN), propõe que, diante de indício de prática de qualquer crime por intermédio da internet, para fins de identificação do suspeito, delegados de polícia e membros do Ministério Público poderão requisitar a provedores de conexão e de aplicações de Internet as informações cadastrais existentes relativas a um dado endereço IP, sem necessidade de autorização judicial.[56] Tais dados cadastrais estariam limitados à qualificação pessoal, à filiação e ao endereço do suspeito, mas o acesso a outras informações poderia ser obtido mediante requerimento a juiz competente. O projeto seguiu para revisão pela Câmara dos Deputados, onde passou a tramitar como PL 5074/2016.[57]

**[nota 53]** Ver BRITO CRUZ, Francisco, et. al., "O que está em jogo na regulamentação do Marco Civil?, InternetLab, 2015, p. 32. Disponível em http://www.internetlab.org.br/wp-content/uploads/2015/08/Report-MCI-v-2-ptbr.pdf. Acesso em 13.09.2015.

**[nota 54]** Ver manifestações nesse sentido em http://participacao.mj.gov.br/marcocivil/pauta/acesso-a-dados-cadastrais-por-autoridades-administrativas/, http://www.internetlab.org.br/pt/internetlab-reporta/internetlab-reporta-consultas-publicas-no-04/ e https://antivigilancia.org/boletim_antivigilancia/consultas/visualizacao . Acesso em: 17.06.2015.

**[nota 55]** Ficha de tramitação do PL 730/2015 disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/123970>. Acesso em 05.05.2017.

**[nota 56]** Texto aprovado pela Comissão Especial do Desenvolvimento Nacional (CEDN) disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=4186074&disposition=inline>. Acesso em 05.05.2017.

**[nota 57]** Ficha de tramitação do PL 5074/2016 disponível em <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2082488>. Acesso em 05.05.2017

### *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: fundados 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".

### *Acesso a comunicações privadas armazenadas*

Como mencionou-se 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,[58] o que dá margem a abusos e aplicações casuísticas.

Para limitar esse tipo de acesso a casos em que é legítimo e apropriado, cabe 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.[59] 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 ao aos elementos concretos do caso investigado.[60] A ordem judicial concedida deve ser minuciosamente fundamentada também nestes termos, em atenção ao art. 93, IX da Constituição Federal.

**[nota 58]** 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.

**[nota 59]** 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).

**[nota 60]** 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.

## CASOS RELEVANTES

### *Ampliando vigilância 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 a vigilância. 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 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 faze-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.[61]

### *Marco Civil limitando a vigilância na Internet*

O Marco Civil da Internet, por outro lado, soma frutos em termos de limitação contra vigilância indevida. A Justiça Federal de São Paulo anulou, em decisão de abril de 2015,[62] 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

**[NOTA 61]** TRIBUNAL DE JUSTIÇA DO RIO GRANDE DO SUL. Agravo de Instrumento n. 70018683508, 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.

**[NOTA 62]** 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/m/jurisprudencias/arquivos/2015/jfsp_00019729120154036100_24042015_KG45KXb.pdf Acesso em: 17.06.2015.

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: A LEI Nº 13.344/16

Em outubro de 2016 foi aprovada a Lei nº 13.344, que dispõe sobre prevenção e repressão ao tráfico interno e internacional de pessoa 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,[63] 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, impõe meros requisitos formais para requisição (indicação de nome da autoridade requisitante, unidade de polícia responsável e número do inquérito) e 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 que podem dar margem a abusos, 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 cria uma clara exceção à 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".

**[NOTA 63]** 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).

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.[64]

## 2.5. VIGILÂNCIA SEM FRONTEIRAS: A EXTRATERRITORIALIDADE DO MARCO CIVIL DA INTERNET

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.[65] 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.[66]

**[NOTA 64]** 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.

**[NOTA 65]** 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: http://direitoeti.com.br/artigos/mlat-x-marco-civil-da-internet/ Acesso em: 25.01.2017.

**[NOTA 66]** Segundo o relator do projeto, Deputado Alessandro Molon, "as modificações foram promovidas tendo em vista que hoje 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

A inclusão desses dispositivos não estancou esse problema - e pode até tê-lo piorado. Uma das forças por trás de bloqueios do aplicativo WhatsApp em todo o país, para além da criptografia, foi justamente a recusa da empresa em fornecer dados a autoridades brasileiras fora dos mecanismos de cooperação internacional.[67]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 intrinsicamente pensados na territorialidade *física*.

## ORIGENS DO PROBLEMA: OS INEFICIENTES ACORDOS DE COOPERAÇÃO MÚTUA E OS CONTORNOS CINZENTOS DE JURISDIÇÃO NA INTERNET

*por 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.[68] 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. [69] 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 coleta 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

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.

**[nota 67]** 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.

**[nota 68]** Ver ACCIOLY, Hildebrando; SILVA, G. E. do Nascimento; CASELLA, Paulo Borba. *Manual de Direito Internacional Público*. 18ª Edição. São Paulo: Saraiva, 2010, p. 321.

**[nota 69]** SOUZA, Carolina Yumi de. "Cooperação jurídica internacional em matéria penal: considerações práticas", *RBCCRIM*, vol. 71, pp. 297-325, 2008, p. 300.

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"[70] entre empresas e autoridades serão frequentes.

## 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. O caso mais emblemático nessa temática é o do Inquérito nº 784/CF, de 2013, em que 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).

**[NOTA 70]** 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: http://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.

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.[71]

Uma expectativa de revisão deste posicionamento pode ser criada a partir de julgados importantes da Justiça Federal. Em 2014, a Yahoo! do Brasil Internet Ltda. foi alvo de ação civil pública proposta pelo Ministério Público Federal (MPF) em razão dos alegados "reiterados descumprimentos de ordens judiciais" determinando o fornecimento de dados de usuários. Segundo argumentou o MPF,[72] seria dever legal da empresa fornecer as informações requisitas, pois a empresa presta serviço no país, ainda que seus provedores estejam localizados no estrangeiro. "O que importa é se detém ou não a informação requisitada judicialmente", argumentou. Como a informação estaria sob total controle das sócias da Yahoo Brasil, domiciliadas nos EUA e com poder sobre a administração da empresa brasileira, haveria possibilidade de (forçar o) fornecimento. A Justiça Federal acolheu a argumentação de defesa, no sentido de que a Yahoo Brasil não tem obrigação de fornecer dados pertencentes a conta de e-mail criada junto a pessoa jurídica diversa (Yahoo! Inc., que administra as contas @yahoo.com). A Yahoo Brasil deve fornecer dados de usuários que efetivamente se cadastraram na versão brasileira do serviço de e-mail (@yahoo.com.br) e anuíram aos seus termos de uso. É o "provedor responsável", terminologia do Marco Civil da Internet, que tem a obrigação de disponibilizar.[73]

A tese da diferenciação entre subsidiária/encarregada de publicidade e matriz/operadora da plataforma também recentemente ajudou o Facebook. Em novembro de 2016, a Justiça Federal do Rio Grande do Sul decidiu que o Ministério Público Federal (MPF) deve 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.[74] 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

**[nota 71]** SUPERIOR TRIBUNAL DE JUSTIÇA, Recurso em Mandado de Segurança nº 46.685/MT. Min. rel. Leopoldo de Arruda Raposo, julg. 26.03.2015.

**[nota 72]** MPF/SP pede condenação da Yahoo! Brasil por desobediência a ordens judiciais, JusBrasil, Procuradoria Geral da República. Disponível em: https://pgr.jusbrasil.com.br/noticias/147375302/mpf-sp-pede-condenacao-da-yahoo-brasil-por-desobediencia-a-ordens-judiciais. Acesso em: 19.01.2017.

**[nota 73]** JUSTIÇA FEDERAL. Processo nº 0012450-95.2014.403.6100. Juíza Federal Sílvia Figueiredo Marques, julg. 13.05.2015.

**[nota 74]** "MPF deve obter dados do Facebook nos EUA por tratado", Jota, 02 de dezembro de 2016, disponível em: http://jota.info/justica/mpf-deve-obter-por-tratado-dados-de-rede-social-diz-juiz-02122016. Acesso em: 19.01.2017.

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.[75] Resta acompanhar se assim permanecerá: a disputa agora se dará no STJ.

## 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 Yahoo em seus relatórios de transparência já publicados que contiveram informações sobre pedidos advindos de autoridades brasileiras.[76] 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.

**QUADRO 5**
PEDIDOS DE DADOS FEITOS POR AUTORIDADES BRASILEIRAS A EMPRESAS DE INTERNET

| | GOOGLE | MICROSOFT | FACEBOOK | YAHOO |
|---|---|---|---|---|
| **2010** | 4.239 | - | - | - |
| **2011** | 2.318 | - | - | - |
| **2012** | 2.777 | - | - | - |
| **2013** | 2.324 | 2.592 | 1.880 | 634 |
| **2014** | 1.468 | 2.461 | 2.519 | 461 |
| **2015** | 1.686 | 2.600 | 2.920 | 520 |
| **2016** | 1.884 | 2.471 | 3.570 | 381 |

Autoria própria a partir de informações divulgadas pelas empresas.

**[NOTA 75]** 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://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.

**[NOTA 76]** As informações estão disponíveis em https://www.google.com/transparencyreport/userdatarequests/BR/, https://www.microsoft.com/about/csr/transparencyhub/lerr/, https://govtrequests.facebook.com/country/Brazil/2016-H2/ e https://transparency.yahoo.com/government-data-requests?tid=22 . Acesso em: 05.05.2017.

## 2.6. INTERCEPTAÇÕES: VIGILÂNCIA LIMITADA NA *TEORIA*, MAS ABRANGENTE NA *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 clássico de vigilância no Brasil. O parágrafo único do art. 1º de tal 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.[77] 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 infração 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,[78] tem prevalecido o entendimento de que a medida pode ser estendida *enquanto* indispensável. A questão está em discussão no STF.[79] O art. 7º

**[NOTA 77]** SUPREMO TRIBUNAL FEDERAL. Ação Direta de Inconstitucionalidade n. 1488-9/DF, Min. Néri da Silveira, julg. em 07.11.1999.

**[NOTA 78]** Ver, do SUPREMO TRIBUNAL FEDERAL, por exemplo, o Habeas Corpus 84.301-SP, Min. rel. Joaquim Barbosa, julg. em 09.11.2004 (disponível em, http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=79542; acesso em 03.08.15) e o Habeas Corpus 83.515-RS, Min. rel. Nelson Jobim, julg. em 16.09.2005 (disponível em http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=AC&docID=79377; acesso em 03.08.15).

**[NOTA 79]** O prazo da realização de interceptações está em discussão no Recurso Extraordinário nº 625263, cujo relator é o Ministro Gilmar Mendes. Já foi reconhecida a repercussão geral do caso.

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 Telefônicas 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. Além disso, elas também preveem que membros do Ministério Público e juízes devem informar mensalmente à Corregedoria-Geral do Ministério Público e à Corregedoria Nacional da Justiça, respectivamente, a quantidade de interceptações em andamento (art. 10 da Resolução nº 36/09 do CNMP e art. 18 da Resolução nº 59/08 do CNJ), com o fim de gerar estatísticas sobre essa prática.

## A PRÁTICA: CULTURA DE INTERCEPTAÇÕES

### *Caso Escher e outros vs. Brasil – Corte Interamericana de Direitos Humanos*

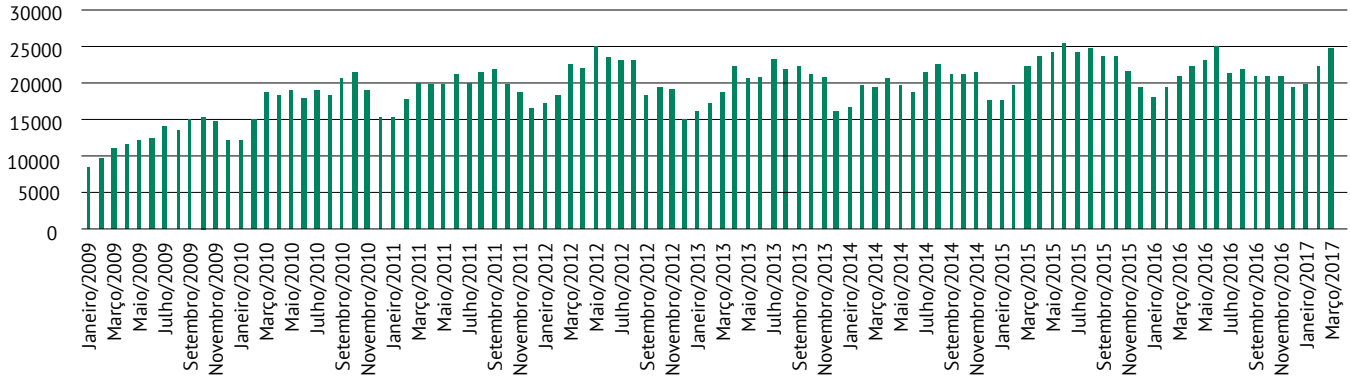
O Brasil foi condenado pela Corte Interamericana de Direitos Humanos (CIDH), em julho de 2009, a indenizar trabalhadores rurais de cooperativas ligadas ao Movimento Sem-Terra, em razão de interceptações telefônicas irregulares realizadas no Estado do Paraná em 1999.[80] As interceptações, que duraram 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 terem sido 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.

**[NOTA 80]** CORTE INTERAMERICANA DE DIREITOS HUMANOS. Caso Escher e outros vs. Brasil. Sentença de 06.07.09. Disponível em http://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.

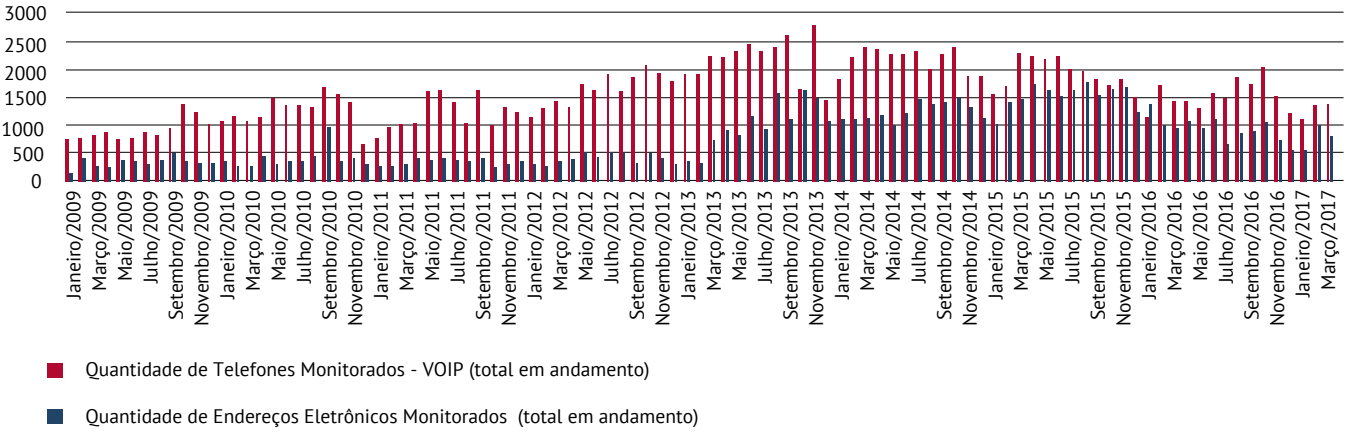
### *Sistema Nacional de Controle de Interceptações*

Em razão da Resolução nº 59/08 do Conselho Nacional de Justiça, juízes de varas criminais de todo o país são obrigados a informar mensalmente à Corregedoria Nacional de Justiça dados relativos a interceptações telefônicas e de sistemas de informática e telemática por meio do "Sistema Nacional de Controle de Interceptações" (SNCI), que recolhe informações sobre ofícios expedidos a prestadoras de serviço, procedimentos instaurados e quantidade de telefones, telefones-VOIP e endereços eletrônicos monitorados. Em 2015, tais dados só puderam ser obtidos pelo INTERNETLAB por meio da Lei de Acesso à Informação; desde fevereiro de 2017, tais dados estão disponíveis publicamente no site do Conselho Nacional de Justiça (CNJ).[81] As estatísticas listadas abaixo se referem às informações do SNCI em 06 de maio de 2017 (ver **ANEXO II**).

#### QUANTIDADE DE LINHAS TELEFÔNICAS MONITORADAS POR MÊS

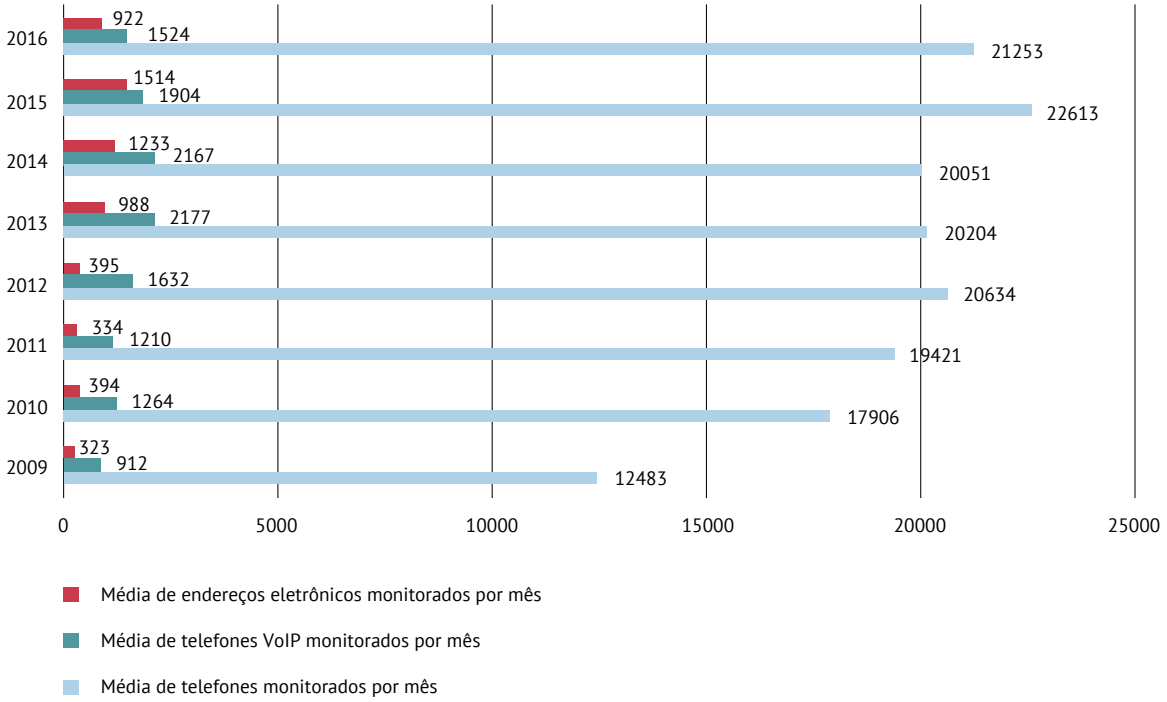



#### TELEFONES VoIP E ENDEREÇOS ELETRÔNICOS MONITORADOS POR MÊS




**[NOTA 81]** Para elaboração deste relatório, o INTERNETLAB iniciou o mesmo procedimento junto à Ouvidoria do CNJ que resultou na divulgação de estatísticas do SNCI que fizeram parte do nosso relatório de pesquisa de 2015. Em novembro de 2016 quando foi feito novo pedido, tais informações ainda foram divulgadas apenas via Ouvidoria (Registro Ouvidoria/CNJ: 176113), com o aviso de que as informações passariam a ser públicas em breve. Pelo menos desde fevereiro de 2017, tais informações podem ser acessadas via http://www.cnj.jus.br/sistemas/interceptacoes-telefonicas (Registro Ouvidoria/CNJ: 186293).

## MÉDIA MENSAL DE ALVOS MONITORADOS POR ANO




Os gráficos mostram que a média mensal de linhas de telefone monitoradas no Brasil ultrapassou 20 mil nos últimos anos. Também se nota que a quantidade de endereços eletrônicos e telefones *voice over* IP monitorados cresceu ao longo dos anos. Em 2016, entretanto, todos os números retraíram um pouco. Em geral, isso poderia apontar para uma tendência positiva, de diminuição das atividades de vigilância do Estado. Todavia, a queda nos números pode também ser decorrência das mudanças nas formas de comunicação cotidianas, que deixaram de estar centradas em ligações telefônicas, abarcando cada vez mais a comunicação por e-mails ou pelo envio de mensagens de texto por aplicativos.[82] No caso das comunicações eletrônicas, a singela queda observada pode estar relacionada à diminuição de pedidos de *interceptação* de comunicações eletrônicas em fluxo e possível aumento de pedidos de quebra de sigilo de comunicações *armazenadas*, já que essas comunicações ficam em trânsito apenas por segundos. Não há estatísticas sobre este tipo de pedido no SNCI, entretanto.

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.

**[NOTA 82]** Uma explicação alternativa ou concorrente para a diminuição das médias em 2016 pode ser o atraso na alimentação do sistema por parte de juízes criminais por todo o país. Os autores levantam esta hipótese porque podem ser notadas acréscimos nos números referentes a período anterior a maio de 2015, quando primeiro fizemos o pedido de acesso a informações do SNCI, quando verificados agora em 2017. As estatísticas divulgadas em 2015 podem ser encontradas em ABREU, Jacqueline de Souza; ANTONIALLI, Dennys. "Vigilância das comunicações pelo 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.

A comparação com outros países tampouco ajuda nessa avaliação, dada a ausência de critérios equivalentes na apresentação das estatísticas. 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 2015, foi de 4.148.[83] Não há informações quanto à quantidade de "interceptações deferidas" no Brasil; o que se sabe é que 12.636 procedimentos criminais novos de interceptação foram instaurados em 2015.[84] Por outro lado, na Alemanha, país com menos da metade da população brasileira, o número de ordens iniciais de interceptação expedidas (*Erstanordnungen*) durante todo o ano de 2015 foi de 18.640.[85] Sobre o Brasil, o que se sabe é que 45.413[86] ofícios iniciais de interceptação foram expedidos a empresas de telecomunicações nesse período e 100.489[87] ofícios no total, o que inclui ofícios de prorrogação de procedimentos já instaurados.

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. Em 2016, a empresa Telefónica, que opera como Vivo no Brasil, divulgou pela primeira vez um relatório de transparência que contém informações sobre pedidos que recebeu de autoridades estatais. Na parte do Brasil, informa que recebeu, em 2015, 326.811 requerimentos de interceptações de comunicações telefônicas e telemáticas.[88] Não fica claro se os "requerimentos" a que a empresa faz referência correspondem ao total de ofícios e ordens que a empresa recebeu ou à soma total de alvos (números de telefone e conexões a Internet) que foram objeto de vigilância. Ainda assim, nota-se que, mesmo representando dados de uma só empresa do mercado de teleco-

**[NOTA 83]** Ver estatísticas disponíveis em http://www.uscourts.gov/statistics-reports/wiretap-report-2015. Acesso em 31.01.2017.

**[NOTA 84]** Ver dados completos do Sistema Nacional de Interceptações obtidos pelo INTERNETLAB no **ANEXO II**. Esse número se refere à quantidade de procedimentos criminais instaurados em 2015 que se dizem „iniciais", conforme indica a tabela, ou seja, que não dizem respeito ao número total de procedimentos instaurados no mês, os quais podem incluir dados do mês anterior. Na indicação da tabela, se referem às informações mensais de 2015 referentes ao item „Total 3", relativas a interceptações telefônicas, somadas às do item Total 9", relativas a interceptações telemáticas.

**[NOTA 85]** Ver estatísticas sob o título "Übersicht Telekommunikationsüberwachung 2015", disponível em: https://www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung.html Acesso em 31.01.17.

**[NOTA 86]** Ver dados completos do Sistema Nacional de Interceptações obtidos pelo INTERNETLAB no **ANEXO II**. Esse número se refere à quantidade de ofícios expedidos em 2015, que se dizem "iniciais", conforme indica a tabela, ou seja, que não dizem respeito ao número total de ofícios expedidos no mês, os quais podem incluir dados do mês anterior. Na indicação da tabela, se referem às informações mensais de 2015 referentes ao item "Total 1", relativas a interceptações telefônicas, somadas às do item "Total 7", relativas a interceptações telemáticas.

**[NOTA 87]** Ver dados completos do Sistema Nacional de Interceptações obtidos pelo INTERNETLAB no **ANEXO II**. Esse número se refere à quantidade total de ofícios expedidos em 2015, novos e de prorrogação. Na indicação da tabela, se referem às informações mensais de 2015 referentes ao item "Total 2", relativas a interceptações telefônicas, somadas às do item "Total 8", relativas a interceptações telemáticas.

**[NOTA 88]** 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.

municações, tal número de requerimentos ultrapassa tanto o número total de ofícios expedidos a empresas (95.481) quanto a soma de telefones (271.364) e telefones-VoIP (22.853) monitorados em 2015 segundo o SNCI.[89]

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*.[90]

## 2.7. VIGILÂNCIA POR MEIO DE INFILTRAÇÕES

### INFILTRAÇÃO POR *SOFTWARE*: O ESTADO COMO HACKER

Em abril de 2015, o jornal *Folha de São Paulo* revelou que a Polícia Federal estaria tentando ampliar o acesso a informações armazenadas em telefones celulares, instalando "vírus" em aparelhos.[91] Isso porque, atualmente, a tecnologia usada em interceptações só daria acesso a mensagens SMS e a ligações, mas não a mensagens trocadas por meio de aplicativos que usam a Internet, como o WhatsApp, cuja utilização tem crescido. A notícia relata ainda que a Polícia Federal "quer que empresas de telefonia adquiram os programas espiões", o que tem sido recebido com resistência em razão dos custos dos programas e da utilização do pacote de dados dos investigados para transferência das informações copiadas. Por meio desses programas, as autoridades teriam capacidade de obter *todas* as informações guardadas em aparelhos e acessar em tempo real o que seu detentor está fazendo. Segundo a reportagem, a polícia quer ter estes poderes de vigilância quando há "autorização judicial".

Notícias mais recentes reforçam o interesse em tecnologias de infiltração – *malwares* – para coleta de dados. Em julho de 2015, a empresa italiana especializada em vender "soluções" de vigilância, isto é, *software* de espionagem eletrônica, para autoridades estatais do mundo inteiro foi *hackeada*. Com isso, vieram a público documentos (sem autenticidade confirmada) que indicam que diversas auto-

**[NOTA 89]** 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://www.bundesjustizamt.de/DE/Themen/Buergerdienste/Justizstatistik/Telekommunikation/Telekommunikationsueberwachung.html) 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.

**[NOTA 90]** 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 http://www.conjur.com.br/2017-jan-29/entrevista-leonardo-sica-criminalista-ex-presidente-aasp . Acesso em: 31.01.2017.

**[NOTA 91]** 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: http://www1.folha.uol.com.br/poder/2015/04/1621459-pf-quer-instalar-virus-em-telefone-grampeado-para-copiar-informacoes.shtml. Acesso em 17.06.15.

ridades policiais brasileiras, o exército, a ABIN, e até a Procuradoria Geral da República, estariam na lista de clientes da empresa.[92] A evidência mais concreta que existe diz respeito aos contatos feitos com a empresa pela Polícia Federal: há troca de e-mails, relatos da realização de treinamento e até certificado de entrega de produto. Em resposta à pedido de acesso à informação feita pelo jornalista João Paulo Vicente, da Motherboard, a Polícia Federal não confirmou a cooperação com o *Hacking Team* nem o uso dos programas de monitoramento, respondendo que estas são informações sigilosas; afirmou, entretanto, que ações de infiltração poderiam ser autorizadas pela Lei de Interceptações (ver **ANEXO III**).[93] De fato, em um dos e-mails,[94] há referência a uma ordem judicial que autorizaria a polícia a utilizar a ferramenta de infiltração por até 15 dias, mesmo prazo previsto na Lei de Interceptações.

Estes acontecimentos evidenciam, de um lado, a necessidade de disciplina legal dos tipos de dados a que se pode ter acesso por meio de quebras de sigilo, para que se respeite o princípio da legalidade e da proporcionalidade na restrição a direitos fundamentais e assim se imponham limites que permitam controle dos poderes de vigilância do Estado sobre as comunicações. A utilização de *malware*, mesmo que dentro de investigação criminal com "interceptação" autorizada por ordem judicial, como são os casos a que as notícias dizem respeito, desperta preocupações que vão além do sigilo das comunicações e afetam a integridade das comunicações e sistemas.[95] 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.

**[nota 92]** Este acontecimento foi tratado aprofundadamente pela Artigo 19 e a Oficina Antivigilância, em contribuição à primeira edição deste relatório do INTERNETLAB. Ver ABREU, Jacqueline de Souza; ANTONIALLI, Dennys. "Vigilância das Comunicações pelo Estado Brasileiro e a proteção a Direitos Fundamentais", São Paulo: InternetLab, 2015, pp. 33-4, disponível em: http://www.internetlab.org.br/wp-content/uploads/2016/01/ILAB_Vigilancia_Entrega_v2-1.pdf .

**[nota 93]** VICENTE, João Paulo, "Ninguém está a salvo no milionário mercado de compra e venda de bugs na Internet", *Motherboard*, 16 de novembro de 2016, disponível em: https://motherboard.vice.com/pt_br/article/mercado-milionario-de-compra-e-venda-de-bugs-aumenta-inseguranca-na-internet . Acesso em: 01.02.2017.

**[nota 94]** Ver o documento vazado pela Wikileaks aqui: https://www.wikileaks.org/hackingteam/emails/emailid/921908 .

**[nota 95]** 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 http://jota.info/uso-de-softwares-espioes-pela-policia-pratica-legal, 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").

## 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 relatório, 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, enquadramento como organização criminosa, e 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).

Em nenhum momento, entretanto, a lei trata especificamente de infiltrações *virtuais* de agentes. À luz das proteções constitucionais, é de se interpretar que as limitações existentes na Lei ao uso dessa medida sejam cabíveis também em meios eletrônicos. Ainda assim, sobram espaços para controvérsias: a distinção entre "rondas virtuais" por plataformas, fóruns e outras informações acessíveis publicamente, de um lado, e por postagens, mensagens, registros e dados com acesso limitado a determinado grupo de pessoas (amigos, seguidores, contatos), de outro, é um dos aspectos que cria dificuldades. Meras atividades de monitoramento de informações publicamente disponíveis não fazem parte das atribuições da polícia judiciária.[96] Buscar ativamente pelo quê investigar na web, portanto, extrapola suas atribuições. Ao mesmo tempo, no campo digital, fica mais difícil controlar *a partir de qual momento* e de *que tipo de engajamento* a atividade é caracterizada como infiltração, a depender de autorização judicial.

### TERRORISTAS NOS JOGOS OLÍMPICOS?

*por Paula Pécora de Barros*

Em julho e agosto de 2016, à época dos Jogos Olímpicos no Rio de Janeiro, a Polícia Federal levou à prisão 15 pessoas, sendo um deles menor de idade, por serem suspeitos de simpatizarem com grupos terroristas.[97] Foram as primeiras ações penais que ocorreram no país pela Lei Antiterrorismo (Lei nº 13.260/2016)[98], e se deram no âmbito da operação Hashtag, conduzida pela Polícia Federal, pela Agência Brasileira de Inteligên-

**[NOTA 96]** Apesar disso, o monitoramento ocorre para esse e outros fins. Ver PORTINARI, Natália. Planalto usa dados de agência para monitorar política em redes sociais, *Folha de São Paulo*, 11 de abril de 2017, disponível em http://www1.folha.uol.com.br/poder/2017/04/1874399-planalto-usa-dados-de-agencia-de-sp-para-monitorar-redes-sociais.shtml?mobile Acesso em: 07.05.2017.

**[NOTA 97]** AFFONSO, Julia; MACEDO, Fausto; BRANDT, Ricardo. Oito viram réus na primeira ação por terrorismo no Brasil, O Estado de São Paulo,19 de setembro de 2016, disponível em: <http://politica.estadao.com.br/blogs/fausto-macedo/oito-viram-reus-na-primeira-acao-por-terrorismo-no-brasil/>. Acesso em 17.01.2017. Os crimes pelos quais eles estavam sendo investigados eram de promoção de organização terrorista (art. 3º da Lei Antiterrorismo) e associação criminosa (art. 288 do Código Penal). Cinco deles respondiam ainda por incentivo de crianças e adolescentes à prática de atos criminosos (art. 244 do Estatuto da Criança e Adolescente), e um deles por recrutamento para organização terrorista (art. 5.º, §1ª, I da Lei n.º13.260/2016 – Lei Antiterrorismo).

cia (ABIN), as Forças Armadas e agências de informação internacionais, para monitorar atividades relacionadas ao terrorismo nas redes sociais, com suspeitas de formação de uma célula do Estado Islâmico no Brasil.[9]

Após as prisões, foi anunciado que havia cerca de cem pessoas sendo monitoradas, suspeitas de também serem simpatizantes de grupos terroristas, pela observação de seu comportamento na Internet, por meio de agentes da Polícia Federal infiltrados e outros métodos que não foram revelados.[100] As pessoas, brasileiras e estrangeiras domiciliadas no Brasil, passaram a ser monitoradas, em grande maioria (em 90% dos casos) por entrarem mais de duas vezes em portais ou propagandas de exaltação a grupos terroristas. Em 10% das vezes, no entanto, chamaram maior atenção da agência de vigilância aquelas que navegaram páginas sobre organizações terroristas, escreveram mensagens com elogios às práticas, ou compartilharam conteúdos com relação ao terror. Os indivíduos presos estavam nesta lista de rastreados que chamaram maior atenção dos agentes de segurança.

Para formar a ordem das prisões, a investigação se deu com base em publicações feitas em perfis das redes sociais Facebook, Twitter e Instagram, e monitoramento das atividades de grupos no WhatsApp e Telegram, criados para trocar informações sobre o Estado Islâmico, a partir de agentes infiltrados,[101] tendo sido inclusive divulgadas fotos das conversas travadas e que levaram às ações,[102] assim como pelo conteúdo de e-mails dos suspeitos, em que demonstraram apoio a atos terroristas e um início de planejamento de atentados para a Olimpíada. Também houve quebra de sigilo de dados e telefônico e a análise do conteúdo de HDs, celulares e outros equipamentos dos suspeitos que foram apreendidos.

Após a investigação, chegou-se à conclusão de que não houve registro de contatos diretos com terroristas por parte de nenhum dos suspeitos, e apenas um deles havia entrado em contato com empresa de armas para comprar um fuzil AK-47, o que não se efetivou. Alguns haviam feito o juramento de lealdade ao Estado Islâmico, por meio de uma gravação do texto repetido pelos membros do EI, encontrado em um site. Foram indiciados por promoção de organização terrorista e atos preparatórios à realização de ataque terrorista.

No início de maio de 2017 houve a condenação dos réus pelos crimes de promoção à organização terrorista (art. 3º da Lei Antiterrorista), recrutamento com o propósito de praticar atos de terrorismo (art. 5º § 1º, I da Lei Antiterrorismo) e associação criminosa (art. 288 do Código Penal), variando-se para cada réu. A Defensoria recorrerá da decisão.[103]

**[nota 98]** \A legislação é alvo de críticas. Ver CHARLEAUX, João Paulo, "O que é e o que não é terrorismo, segundo a lei sancionada por Dilma", *Nexo*, 21 de março de 2016, disponível em: https://www.nexojornal.com.br/expresso/2016/03/21/O-que-é-e-o-que-não-é-terrorismo-segundo-a-lei-sancionada-por-Dilma Acesso em: 03.02.2017.

**[nota 99]** ONOFRE, Renato; CARVALHO, Cleide. Grupo terrorista discutiu fazer ataque químico na Olimpíada do Rio, *O Globo*, 02 de setembro de 2016. Disponível em: <http://oglobo.globo.com/rio/grupo-terrorista-discutiu-fazer-ataque-quimico-na-olimpiada-do-rio-20040958>. Acesso em 18.01.2017.

**[nota 100]** CANALTECH, "Polícia Federal teria monitorado WhatsApp de suspeitos de terrorismo", 21 de julho de 2016, disponível em: <https://canaltech.com.br/noticia/seguranca/policia-federal-teria-monitorado-whatsapp-de-suspeitos-de-terrorismo-74213/>. Acesso em 18 jan, 2017.

**[nota 101]** DESIDÉRIO, Mariana, "PF usou infiltrado contra ataque na Olimpíada, diz jornal", *EXAME*, 23 de julho de 2016, disponível em: <http://exame.abril.com.br/brasil/pf-usou-infiltrado-contra-ataque-na-olimpiada-diz-jornal/>. Acesso em 18 jan, 2017.

**[nota 102]** KÖNIG, Mauri, "Grupo simpatizante ao terrorismo cogitou usar arma química nos Jogos do Rio", *Folha de São Paulo*, 02 de setembro de 2016, disponível em: <http://www1.folha.uol.com.br/esporte/olimpiada-no-rio/2016/09/1809421-grupo-simpatizante-ao-terrorismo-cogitou-usar-arma-quimica-nos-jogos-do-rio.shtml>. Acesso em 01.03.2017.

**[nota 103]** JORDÃO, Rogério Pacheco, "Um fiasco olímpico", *A Pública,* 04 de maio de 2017, disponível em: http://apublica.org/2017/05/um-fiasco-olimpico/ . Acesso em: 05.05.2017.

Outras normativas já utilizadas como base de infiltrações virtuais são a Garantia da Lei e da Ordem, publicada via portaria normativa do Ministério da Defesa nº 186 de 31 de janeiro de 2014, e a Política Nacional de Inteligência, fixada pelo Decreto nº 8.793 de 29 de junho de 2016, as quais são aplicáveis a agentes *militares* ou *de inteligência*. É indiscutível que operações destinadas à coleta de "conhecimentos"[104] envolvem a atuação de agentes em campo. Entretanto, os regramentos citados são apenas gerais, não regulando detalhadamente as atividades de infiltração de agentes. Muito menos na Internet. É de se esperar que operações envolvendo infiltrados atendam aos objetivos, diretrizes e limites pré-estabelecidos para as atividades de inteligência e contrainteligência, mas como o exercício dessas atividades são marcadas pela obscuridade, é no mínimo complicada a averiguação do respeito aos limites legais e constitucionais.

## O MILITAR QUE FINGIU SER MANIFESTANTE NO TINDER

*por Paula Pécora de Barros*

Outro caso envolvendo a atuação de agentes do Estado em redes sociais foi o que levou à prisão de 21 jovens, detidos à caminho de uma manifestação em São Paulo. A história se tornou notória quando se descobriu que as prisões decorreram da denúncia de um oficial do Exército infiltrado no grupo de manifestantes.

O militar Willian Pina Botelho se apresentava como Balta Nunes nas redes sociais e no aplicativo de relacionamentos Tinder, dizendo ser "militante da esquerda", para se aproximar de jovens contrários ao atual governo federal e participantes nos protestos que estavam ocorrendo na cidade. Por meio de uma militante que conheceu no Tinder, foi incluído em um grupo de WhatsApp que contava com cerca de 40 manifestantes se organizando para irem juntos a um ato no dia 4 de setembro de 2016 contrário ao governo do presidente Michel Temer. O grupo, composto majoritariamente por jovens de 20 anos que não se conheciam, combinou de se encontrar no metrô Consolação, para de lá irem juntos ao protesto. Após o encontro, o militar, disfarçado de manifestante, sugeriu que fossem até o Centro Cultural São Paulo, onde poderiam encontrar outras pessoas indo à manifestação. No novo local, o grupo, que estava apenas esperando mais manifestantes sem causar tumulto, foi abordado por agentes da Polícia Militar e por um helicóptero. Todos os jovens foram presos e conduzidos à delegacia, exceto "Balta", que foi colocado sozinho em outra viatura mas não chegou à delegacia.

Após a suspeita dos manifestantes de que ele seria um agente disfarçado, a repercussão na mídia fez com que fosse identificado como Botelho, o oficial do Exército, o qual, segundo o portal da Transparência[105], está em atuação desde 1998. A atuação do militar como infiltrado foi, em um primeiro momento, negada pelo Estado. Posteriormente, o Exército reconheceu que era realmente o militar, negando, no entanto, que ele estaria atuando infiltrado.

Em 09 de setembro de 2016, foi aberta uma investigação[106] sobre o envolvimento do capitão Willian Pina Botelho, mas foi apenas em novembro que o Exército admitiu realizar "operações de inteligência" permanentes em "manifestações de rua", mas sem confirmar que usavam militares infiltrados. Tal atuação

**[nota 104]** Termo utilizado na área. Pelo Decreto nº 8.793/2016, "atividade de inteligência" se refere ao exercício permanente de ações especializadas, voltadas para a produção e difusão de conhecimentos, com vistas ao assessoramento das autoridades governamentais nos respectivos níveis e áreas de atribuição, para o planejamento, a execução, o acompanhamento e a avaliação das políticas de Estado.

**[nota 105]** PORTAL DA TRANSPARÊNCIA. Governo Federal Ministério da Transparência, Fiscalização e Controladoria-Geral da União.Servidores civis e militares do poder Executivo Federal. http://www.portaldatransparencia.gov.br/servidores/Servidor-DetalhaServidor.asp?IdServidor=1880960

**[nota 106]** "MP vai investigar suposto abuso da polícia em protestos contra Temer", *O Globo*, 06 de setembro de 2016, disponível em: <http://oglobo.globo.com/brasil/mp-vai-investigar-suposto-abuso-da-policia-em-protestos-contra-temer-20063992> Acesso em: 19.01.2017.

de inteligência estaria legitimada pela norma de Garantia de Lei e da Ordem (GLO)[107] , que regra a operação militar realizada pelas Forças Armadas para preservar a ordem pública, incolumidade das pessoas e do patrimônio a qual tem sido criticada desde sua propositura, por permitir condutas autoritárias e arbitrárias, definindo como legítima a atuação das Forças Armadas nas situações que caracterizam "perturbação da ordem", conceito indefinido.

O procedimento investigatório preliminar foi arquivado em dezembro pela Procuradoria da Justiça Militar em São Paulo, órgão do Ministério Público Federal. O promotor Luis Antonio Grigoletto, responsável para analisar o caso, entendeu que o capitão atuava em acordo com o Decreto Presidencial de 31 de agosto de 2016, acionado para autorizar o emprego das Forças Armadas para garantir a ordem no dia do revezamento da Tocha Paraolímpica dos Jogos Rio 2016, que passaria justamente no dia 04 de setembro em São Paulo.[108] Cabe observar, entretanto, que Botelho já estava infiltrado nas redes sociais como "Balta" dias antes.

## ENQUANTO ISSO, NO LEGISLATIVO...

*por Beatriz Kira*

O plenário do Senado Federal, em 5 de abril de 2017, aprovou o Projeto de Lei do Senado (PLS) 100/2010, que altera o Estatuto da Criança e do Adolescente (Lei 8069/1990) para incluir seção específica acerca da infiltração de agentes de polícia na Internet para investigação de crimes contra a dignidade sexual da criança e do adolescente. A proposta define normas para que agentes policiais possam se infiltrar anonimamente na internet, sem que essa conduta configure crime por ocultação de identidade. Segundo o projeto, a infiltração poderá ser feita a pedido do Ministério Público ou de representação do delegado de polícia e dependerá de autorização judicial fundamentada. A infiltração somente poderá ocorrer se a prova não puder ser obtida por outros meios legais e terá duração máxima de 90 dias, mas poderá ser renovada pelo prazo máximo de 720 dias, caso demonstrada efetiva necessidade. O texto, entretanto, não define o que será entendido como "infiltração", para fins de aplicação da futura lei. Assim, não há clareza se essa infiltração diria respeito à atuação em redes sociais, grupos e fóruns online, por exemplo, ou se também poderia ser utilizada para justificar o uso de dispositivos como spywares por parte das autoridades.[110] Em 08 de Maio de 2017, o projeto virou a lei federal nº 13.441.

**[nota 107]** TOMAZ, Kleber, "Exército admite realizar 'operações de inteligência' em manifestações de rua", *G1*, 23 de setembro de 2016, disponível em: <http://g1.globo.com/sao-paulo/noticia/2016/09/exercito-admite-realizar-operacoes-de-inteligencia-em-manifestacoes-de-rua.html>. Acesso em 20.01.2017.

**[nota 108]** "Justiça militar arquiva investigação sobre capitão 'infiltrado' em protesto em SP", *G1*, 26 de dezembro de 2016, disponível em: <http://g1.globo.com/sao-paulo/noticia/justica-militar-arquiva-investigacao-sobre-capitao-infiltrado-em-protesto-em-sp.ghtml>.

**[nota 109]** Ficha de tramitação do PLS 100/2010 disponível em: <http://www25.senado.leg.br/web/atividade/materias/-/materia/96360>. Acesso em 05.05.2017.

**[nota 110]** Texto final enviado à sanção presidencial disponível em: <http://legis.senado.leg.br/sdleg-getter/documento?dm=5224875>. Acesso em 05.05.2017.

## 2.8. VIGILÂNCIA *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 produzem conhecimentos de interesse das atividades de inteligência (art. 2º), especificadas no art. 4º do Decreto nº 4.376/02, entre eles a Casa Civil e o Gabinete de Segurança Institucional da Presidência da República, Ministérios da Justiça, da Defesa, das Relações Exteriores, da Saúde, da Fazenda, da Ciência e Tecnologia, entre outros, e órgãos a eles relacionados como a Polícia Federal, o Departamento Penitenciário Nacional, o Departamento de Cooperação Jurídica Internacional, as Forças Armadas, a Receita Federal e o Banco Central. Órgão central constitui a Agência Brasileira de Inteligência (ABIN), a quem compete planejar, executar, supervisionar e controlar 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 ABIN pode ter acesso a dados obtidos por outras autoridades por meio da SISBIN. 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, incluído em 2008, previu que a ABIN poderá ter representantes de órgãos do SISBIN junto a seu Departamento de Integração do SISBIN, os quais "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). De fato, a Política Nacional de Inteligência também estabelece como diretriz do SISBIN o "compartilhamento de dados e conhecimentos" entre os diversos organismos estatais.[111]

Com isso, é possível à ABIN ter acesso a informações e dados a princípio protegidas pelo sigilo das comunicações, o que amplia as possibilidades de vigilância do Estado brasileiro. A despeito de não poder realizar diretamente interceptações, por exemplo, por não ter sido contemplado o fim de inteligência na Constituição nem na Lei das Interceptações,[112] o acesso a dados por meio de cooperação não

**[NOTA 111]** 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.

**[NOTA 112]** 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

estaria descartado. Caso revelado pelo jornal *Folha de São Paulo* em 2008 revela esse tipo de acesso indireto da ABIN a comunicações interceptadas disponíveis no sistema Guardião da Polícia Federal.[113] Caso a Receita Federal disponha de documentos fiscais de empresas de telefonia em seus bancos de dados, à ABIN também estaria aberta a possibilidade de ter acesso a registros telefônicos de usuários.

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). Contudo, a falta de transparência sobre a forma como se dá a cooperação pelo SISBIN impede a avaliação rigorosa da ABIN em termos de vigilância, e cobre a sua atuação de obscuridade e incertezas.

## "MOSAICO" DA ABIN: MENOS TRANSPARÊNCIA, MAIS OBSCURIDADE

Em junho de 2013, o jornal *Estado de São Paulo* revelou que a ABIN, por meio de "sistema *online* de acompanhamento de temas" definidos pelo Gabinete de Segurança Institucional (GSI), o "Mosaico", estaria monitorando redes sociais como Facebook, Twitter, Instagram e WhatsApp para acompanhar a movimentação de manifestantes em meio a uma onda de protestos de rua que ocorria em todo o país naquele período.[114] O objetivo seria tentar "antecipar o roteiro e o tamanho dos protestos, infiltrações de grupos políticos e até supostos financiamentos dos eventos". A tomada de conhecimento por parte do Estado de comunicações públicas não é ilegal no Brasil e, por isso, o monitoramento da ABIN, a princípio, não é irregular. Há lugar aqui, contudo, para dois comentários. Em primeiro lugar, a revelação do jornal inclui a acusação de que mensagens *privadas*, como as que são veiculadas pelo WhatsApp, também estariam sendo monitoradas, o que caracteriza interceptação do fluxo de comunicações para a qual a ABIN não detém competência legal. Pode também, outra vez, sugerir a atuação nebulosa de infiltrados. Em segundo lugar, a notícia evidencia a necessidade de transparência acerca do funcionamento do programa "Mosaico" da ABIN, de sua abrangência e finalidades, essencial para o controle efetivo da vigilância do Estado brasileiro sobre as comunicações.[115]

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: http://www.abin.gov.br/modules/mastop_publish/?tac=Perguntas_Frequentes (Acesso em: 31.07.2015). 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/cr0709200802.htm . Acesso em: 31.07.2015.

**[NOTA 113]** 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.

**[NOTA 114]** RIZZO, Alana; MONTEIRO, Tania, "Abin monta rede para monitorar internet", *O Estado de São Paulo*, 19 de junho de 2013, disponível em: http://sao-paulo.estadao.com.br/noticias/geral,abin-monta-rede-para-monitorar-internet,1044500 Acesso em: 17.06.2015.

**[NOTA 115]** Essas preocupações foram exploradas por especialistas em REVISTA GALILEO, "Mosaico, o 'Prism' brasileiro", sem data de publicação, disponível em: http://revistagalileu.globo.com/Revista/Common/0,,EMI-339490-17770,00-MOSAICO+O+PRISM+BRASILEIRO.html Acesso em: 17.06.2015.

# 3 RECOMENDAÇÕES

O presente relatório apresentou leis e práticas brasileiras de vigilância das comunicações. Foram identificados aspectos positivos da legislação e salientados os pontos mais problemáticos que a envolvem, seja na letra da lei ou na sua aplicação na prática. Cabe agora fazer recomendações. Para tanto, serão utilizados 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.[116]

## 3.1. PRINCÍPIOS INTERNACIONAIS SOBRE A APLICAÇÃO DE DIREITOS HUMANOS À VIGILÂNCIA DAS COMUNICAÇÕES

### 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 com os direitos à privacidade e com a 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.

**[NOTA 116]** https://pt.necessaryandproportionate.org/text

### 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 mecanismos de fiscalização 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 propósitos de vigilância estatais.

### 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 garantem que os standards de maior proteção à privacidade devem ser 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.

## 3.2. RECOMENDAÇÕES ESPECÍFICAS

1. ***Promover uma mudança na cultura jurídica, com a formação de estudantes em temas de privacidade, sigilo das comunicações e liberdade de expressão, principalmente quando associados à tecnologia, e familiarizar operadores e futuros operadores do direito sobre os princípios internacionais sobre a aplicação dos direitos humanos na vigilância das comunicações;***

Um dos problemas básicos identificados neste estudo foi a adoção de interpretações restritivas dadas a direitos fundamentais da Constituição brasileira, que ameaçam, na prática, a efetividade da proteção que esses direitos garantem. Isso conduz a menores proteções a dados de usuários de serviços de telecomunicações, mesmo quando exigem ordem judicial para serem acessados. A quantidade de telefones interceptados no Brasil e o crescente número de *emails* monitorados, a despeito da impossibilidade de se retirar conclusões concretas sobre sua grandeza na ausência de mais informações, sugerem que concretizações teóricas de princípios em lei podem não se refletir na prática. A promoção de ensino, esclarecimento e debate aumentará a sensibilidade a essas questões e permitirá o aumento de decisões informadas em matéria de vigilância, o que é um pressuposto para a efetiva observância do princípio da autoridade judicial competente. Isso pode ser feito com a inclusão de disciplinas que abordem essas questões no currículo das faculdades de Direito

e com a realização de cursos e palestras de atualização voltados aos operadores do direito, como membros do Poder Judiciário e do Ministério Público.

2. ***Revisar os termos das Resoluções da ANATEL que possuem impacto em termos de vigilância sobre as comunicações e exigir transparência em sua atuação fiscalizatória;***

As resoluções da ANATEL instituem obrigações de identificação dos usuários, de guarda de dados e de possuir infraestrutura de vigilância, e conferem prerrogativa de acesso direto a dados, com o que limitam direitos fundamentais. Seus termos precisam ser, por isso, revistos. A Resolução nº 426/05 da ANATEL, aplicável à telefonia fixa, não cumpre requisitos de clareza e precisão sobre dados a serem guardados, ao instituir tal obrigação e sobre as autoridades que podem ter acesso a eles, o que é um problema grave à luz do princípio da legalidade. Além disso, a guarda de registros por resolução para fins de regulação das telecomunicações deve se restringir ao estritamente necessário ao exercício dessa finalidade, para que esteja de acordo com os princípios do fim legítimo e da necessidade. As obrigações de guardas de dados fixadas em 5 anos devem ser reconsideradas. Na Europa, os prazos previstos são muito inferiores: na já derrubada Diretiva de Retenção de Dados eram de seis meses a dois anos[117]; atualmente, na Alemanha, há obrigações de guarda por 10 semanas.[118] Paralelamente, está em desacordo, no mínimo, com o princípio da transparência, a possibilidade de acesso direto a registros telefônicos, através da integração de sistemas da ANATEL com os das prestadoras. Há de se prever com clareza as hipóteses em que o acesso ocorrerá.

3. ***Monitorar o andamento de ações direta de inconstitucionalidade propostas perante o Supremo Tribual Federal e investir em estratégias de incidência sobre seus resultados, como pela elaboração de amici curiae;***

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.

**[nota 117]** Ver Diretiva 2006/24/EC sobre retenção de dados gerados e processados na prestação de serviços de telecomunicações, disponível em http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF. Acesso em 03.08.2015.

**[nota 118]** A Alemanha reintroduziu a guarda obrigatória de metadados gerados na utilização de serviços de telecomunicações em outubro de 2015. Ver notícia do parlamento alemão em https://www.bundestag.de/dokumente/textarchiv/2015/kw42_de_vorratsdatenspeicherung/391654. Acesso em 06.05.2017. Sobre o tema, ver também ABREU, Jacqueline de Souza, "Uma nova lei de retenção de dados para a Alemanha – dessa vez constitucional?", in: Blog InternetLab, publicado em 23 de abril de 2015, disponível em http://www.internetlab.org.br/pt/opiniao/uma-nova-lei-de-retencao-de-dados-para-a-alemanha-dessa-vez-constitucional/ Acesso em 03.08.2015.

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 sobre isso). A Lei dos Crimes de Lavagem de Dinheiro e as recentes 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. Intervenção nesses processos é imprescindível.

4. ***Regular hipóteses e requisitos de acesso a metadados gerados na telefonia em lei específica;***

O acesso a registros telefônicos não pode ter o tratamento improvisado que encontrou na Lei das Organizações Criminosas, que apenas o deixou mais suscetível a abusos e ainda mais distante do respeito aos princípios internacionais aplicáveis em matéria de vigilância. O acesso a metadados da telefonia[119] 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. Somente assim se chegaria mais perto do respeito aos princípios internacionais.

5. ***Monitorar a aplicação do Marco Civil da Internet, acompanhar o processo de elaboração do seu regulamento e revisar a constitucionalidade de seu art. 15;***

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. Esses ganhos teóricos ainda precisam se tornar práticos. O monitoramento da aplicação do Marco Civil é, portanto, essencial.

**[nota 119]** Ver a inúmera quantidade de diferentes metadados relacionados ao uso de telefonia móvel em TEIXEIRA, Lucas, Quais dados seu celular e a rede móvel coletam?, *Boletim Antivigilância*, n. 15, 02 de maio de 2017, disponível em: https://antivigilancia.org/pt/2017/05/dados-infra/ Acesso em: 06.05.2017.

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, se não declarada a inconstitucionalidade em si de tal dispositivo, 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.

6. ***Monitorar a aplicação da Lei de Interceptações Telefônicas a novas técnicas de vigilância e influenciar o seu uso em novos casos;***

O relatório mostrou que a Lei das Interceptações Telefônicas se aplica não só a interceptações telefônicas, mas também a telemáticas. Mais que isso, também indicou que tem se buscado estender a aplicação da Lei de para novos casos: o da infecção de *malware* em celulares e computadores, como mostraram a notícia citada e o relato sobre a aparente cooperação de autoridades brasileiras com o *Hacking Team*. 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. Enquanto isto não ocorre, e na medida em que se tiver notícia de casos, a aplicação da Lei de Interceptações pode e deve ser influenciada pela participação em processos judiciais, como com a intervenção por *amici curiae*.

7. ***Realizar estudos empíricos acerca das práticas de autoridades policiais e do Ministério Público de requisição de dados cadastrais e pedidos de quebra de sigilo de metadados; elaborar estatísticas acerca da quebra de sigilo de metadados; estender e dar publicidade às informações recolhidas pelo Sistema Nacional de Controle de Interceptações;***

Reformas legislativas recentes conferem 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.[120] Isso parece sugerir que *(i)* a investigação criminal no Brasil é forte-

**[nota 120]** Vejam-se o Projeto de Lei 8.040/14 da Câmara dos Deputados, que inclui prerrogativa de acesso direta a dados cadastrais de usuários de Internet à Polícia Federal, disponível em http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=623798, e o Projeto de Lei 494/08 do Senado Federal, que estende obrigação de guardas de registros de conexão à Internet e permite acesso por mera requisição a autoridades policiais e ao Ministério Público a informações cadastrais e "dados de conexão" quando se tratar de investigações "que envolvam crianças e adolescentes", disponível em https://www25.senado.leg.br/web/atividade/materias/-/materia/88862, já remetido à Câmara. Acesso em 07.05.2017.

mente 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.

Paralelamente, é imprescindível que dados do Sistema Nacional de Controle de Interceptações da Corregedoria Nacional de Justiça sejam ampliados: não há informações sobre número total de pedidos de interceptações feitos, nem o de pedidos de interceptações deferidos, apenas o de procedimentos instaurados, o que impede a avaliação completa dessa prática. O controle sobre as interceptações não pode ser exercido sem publicidade sobre seus números. Além dessa ampliação, é necessário aventar a criação de um sistema abrangente, incluindo estatísticas sobre quebras de sigilo de comunicações armazenadas e metadados. O decreto 8.771/16, que regulamentou o Marco Civil da Internet, impôs a órgãos da administração pública federal o dever de anualmente publicar estatísticas sobre requisições de dados cadastrais a provedores de conexão e de aplicações (art. 12). Apesar de acertado, este passo ainda é singelo.

### 8. *Fomentar discussões sobre uma possível reforma dos acordos internacionais de cooperação mútua em matéria penal;*

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 relatório, 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. Diante disso, enquanto em alguns países avançam discussões sobre as possibilidades de reforma e aprimoramento desses mecanismos, no Brasil, pouco se tem discutido a respeito disso.

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.[121] Isso exige um urgente 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.

**[nota 121]** Ver, por exemplo, ARAS, Vladimir, "O Facebook não vai dar 'like'", *Blog do Vlad*, 24 de julho de 2016, disponível em: https://vladimiraras.blog/2016/07/24/o-facebook-nao-vai-dar-like/ Acesso em: 05.05.2017. As propostas de Vladimir Aras, secretário de cooperação judiciária internacional do Ministério Público Federal, podem servir para começar um diálogo crítico sobre o tema no Brasil, que venha a engajar outros setores interessados.

9. ***Pressionar por transparência na atuação para fins de inteligência e segurança nacional, criar balizas para transferência de dados dentro do SISBIN e aumentar o controle;***

Pouco se estuda a atuação da ABIN e do SISBIN no Brasil. Do controle exercido por 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.[122] Recomendação básica parece ser aqui 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 relatório 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 encontra cooperação pelo SISBIN com 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 – podem estar sendo desvirtuados para a sua utilização para fins de inteligência.

10. ***Acompanhar a tramitação dos projetos de lei que se referem à proteção de dados pessoais e promover o debate público a respeito de sua aplicação para atividades de vigilância desempenhadas pelo Estado.***

Em outubro de 2016, a Câmara dos Deputados instaurou uma Comissão Especial para apreciar os projetos de lei (PL) no. 4060/2012, de autoria do dep. Milton Monti (PR-SP), no 6291/2016, de autoria do dep. João Derly (REDE-RS), e no 5276/2016, proposto pelo Poder Executivo. Os projetos dispõem sobre um regime de proteção de dados pessoais no Brasil, matéria ainda não completamente regulamentada em nível infraconstitucional.

Embora as atividades de tratamento de dados realizadas "para fins exclusivos de segurança pública, de defesa nacional, de segurança do Estado ou de atividades de investigação e repressão de infrações penais" estejam fora do escopo de incidência de alguns desses projetos (art. 4º, III, PL nº 5276/2016), os princípios gerais de proteção e os direitos que estabelecerem poderão ser aplicados subsidiária ou complementarmente a essas atividades (art. 4º, § 1º, PL no 5276/2016). Por essa razão, participar dos debates públicos relativos à sua tramitação pode ser fundamental para garantir que a regulamentação inclua dispositivos que consagrem princípios como finalidade, necessidade e adequação, que por sua vez, podem representar importantes balizas também para as atividades de coleta e tratamento de dados pessoais desempenhadas pelo Estado.

**[NOTA 122]** O setor de inteligência ganhou maior evidência com a Copa do Mundo de 2014 no Brasil e continuará importante com a realização das Olimpíadas de Verão em 2016 no Rio de Janeiro. Sobre a atuação, ver VALENTE, Rubens, "Ameaça de bomba na Copa mobilizou inteligência e deixou Dilma apreensiva", *Folha de São Paulo*, 14 de junho de 2016, disponível em http://www1.folha.uol.com.br/esporte/2015/06/1641861-ameaca-de-bomba-na-copa-mobilizou-inteligencia-e-deixou-dilma-apreensiva.shtml . Acesso 31.07.2015.

# 4
# ANEXOS

## 4.1. ANEXO I

| Dados do Pedido | |
|---|---|
| Protocolo | 53850000054201787 |
| Solicitante | Jacqueline de Souza Abreu |
| Data de Abertura | 17/01/2017 12:05 |
| Orgão Superior Destinatário | MC – Ministério das Comunicações |
| Orgão Vinculado Destinatário | ANATEL – Agência Nacional de Telecomunicações |
| Prazo de Atendimento | 06/02/2017 |
| Situação | Respondido |
| Status da Situação | Acesso Concedido (Resposta solicitada inserida no e-SIC) |
| Forma de Recebimento da Resposta | Pelo sistema (com avisos por email) |
| Resumo | Informações sobre acesso direto a dados junto a prestadoras |
| Detalhamento | Prezados,<br><br>O jornal Folha de São Paulo revelou em 2011 as intenções da ANATEL de possuir acesso direto e sistemático a dados gerados na prestação de serviços de telecomunicações por meio da construção de infraestrutura que permitisse acesso online irrestrito à ANATEL, com o objetivo de modernizar sua fiscalização (http://www1.folha.uol.com.br/fsp/mercado/me1901201103.htm).<br><br>Nesta linha, o art. 38 da Resolução nº 596/12 da ANATEL instituiu as obrigações às prestadoras de serviços de telefonia de fornecer dados, permitir o acesso e disponibilizar o acesso online a aplicativos, sistemas, recursos e facilidades tecnológicos utilizados por elas “para coleta, tratamento e apresentação de dados, informações e outros aspectos”, confirmando as intenções da agência.<br><br>Tendo isso em vista, solicito as informações relativas ao programa de compartilhamento de informações entre prestadoras e a ANATEL.<br>1) Quais informações são compartilhadas (informações cadastrais de clientes? registros telefônicos? valores de chamada?)?<br>2) Que informações fazem parte de "documentos fiscais" que podem ser fiscalizados pela ANATEL? Registros telefônicos de clientes constam em documentos fiscais?<br>3) Especificação do que consistem informações "de natureza técnica, operacional, econômico-financeira, contábil ou outras pertinentes" (Art. 38).<br>4) Quando informações são compartilhadas entre prestadoras e a ANATEL? O acesso é contínuo à discricionariedade da ANATEL (direto) ou depende da configuração de situações específicas e/ou de atuação da prestadora e/ou do usuário afetado?<br>5) Por que meio se dá o compartilhamento e o acesso aos dados? Há utilização de software? Se sim, qual?<br><br>Obrigada. |

| Dados da Resposta | |
|---|---|
| Data de Resposta | 06/02/2017 15:24 |
| Tipo de Resposta | Acesso Concedido |
| Classificação do Tipo de Resposta | Resposta solicitada inserida no e-SIC |
| Resposta | Prezada Jacqueline de Souza Abreu:<br><br>Preliminarmente, acerca do teor da reportagem veiculada em (http://www1.folha.uol.com.br/fsp/mercado/me1901201103.htm), cumpre informar que a Anatel não monitora nem coleta (grava) os conteúdos de chamadas telefônicas. Eventualmente pode ocorrer a necessidade se obter informações de caráter técnico, sem conteúdo de dados pessoais, relacionadas a chamadas telefônicas como, por exemplo, aquelas que |

permitem avaliar se estão ocorrendo cobranças de valores indevidos dos usuários. Esse tipo de informação é requisitado às operadoras dentro de atividades de fiscalização para atendimento a diversos tipos de demandas, vindas, por exemplo, do Poder Judiciário, do Ministério Público, ou mesmo decorrentes de denúncias de irregularidades registradas pelo público em geral por meio dos diversos canais de comunicação com a Agência (Call Center, denúncias escritas, reclamações registradas pela internet entre outros).

Há outros tipos de atividades de fiscalização e acompanhamento sobre a qualidade da prestação dos serviços de telecomunicações que requerem da Agência a obtenção, no âmbito das operadoras, de dados para cálculos de indicadores de desempenho de redes, tais como taxa de queda de ligação, taxa de completamento de chamadas e ocorrências de interrupção de serviço. As informações obtidas nesses casos são fornecidas de forma agregada, sem qualquer detalhamento das chamadas ocorridas.
A título de exemplificação, destaca-se que por meio desse tipo de ação da Agência são coletados dados que alimentam o aplicativo da Anatel que disponibiliza para o público em geral os indicadores de qualidade do serviço móvel pessoal.

Quanto às perguntas feitas, seguem os respectivos esclarecimentos:

1) Quais informações são compartilhadas (informações cadastrais de clientes? registros telefônicos? valores de chamada?)?
Informações registradas nos diversos sistemas de informação das operadoras que permitem à Anatel aferir se seus serviços prestados atendem aos requisitos de qualidade e desempenho conforme a regulamentação vigente. Exemplificativamente, são informações sobre desempenho e tráfego das redes; verificação de taxas de utilização das redes e serviços; verificação de interrupção de serviços; identificação de eventos de alarmes e falhas; dados dos sistemas de Bilhetagem/Faturamento e que tratam os registros de chamadas (denominados Call Detailed records ou CDRs) para emissão das faturas; Consultas às tabelas de planos de serviços oferecidos pela operadora ; sistemas usados nas centrais de atendimento (Call Centers) para interação com os usuários ; Sistemas de cadastro de clientes que são acessados pelos atendentes de Call Center; Sistemas de gerenciamento da plataforma de Call Center.

2) Que informações fazem parte de "documentos fiscais" que podem ser fiscalizados pela ANATEL? Registros telefônicos de clientes constam em documentos fiscais?

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.

3) Especificação do que consistem informações "de natureza técnica, operacional, econômico-financeira, contábil ou outras pertinentes" (Art. 38).

Informações de natureza técnica e/ou operacional são aquelas que permitem à Anatel acompanhar o desempenho dos serviços prestados para aferição dos níveis de qualidade ou outros parâmetros. São informações agregadas que não trazem em si identificação dos usuários. Inclui obter os dados gerados pelos diversos sistemas de informação utilizados pelas operadoras na prestação dos serviços. Alguns exemplos incluem os dados sobre o tráfego, congestionamento, interrupção, taxas de queda de ligação, taxas de completamento de chamadas, quantidade de reclamações de usuários, taxas de sucesso na conexão de dados, quantidade de chamadas nos telefones de uso público, inventário da infra-estrutura das redes de prestação dos serviços, velocidades das

| | |
|---|---|
| | conexões de banda larga fixa, quantidade de assinantes (usuários) dos serviços de telefonia fixa, móvel, banda larga e TV por assinatura, entre outras informações agregadas. Muitas destas informações agregadas coletadas junto às operadoras estão disponíveis para acesso público na própria página da Anatel na internet no endereço: http://www.anatel.gov.br/dados/.<br><br>Informações de natureza econômico-financeira e/ou contábil incluem dados sobre receitas operacionais brutas e líquidas, tais como balancetes, Demonstrações de Resultado, Balanço Patrimonial, declarações ao SPED Contabil e Fiscal da Receita Federal do Brasil, informações sobre a composição do controle societário das empresas, dados da contabilidade. Essas informações são obtidas por meio de Requerimentos de Informações.<br><br>4) Quando informações são compartilhadas entre prestadoras e a ANATEL? O acesso é contínuo à discricionariedade da ANATEL (direto) ou depende da configuração de situações específicas e/ou de atuação da prestadora e/ou do usuário afetado?<br><br>As solicitações de informações junto às operadoras por parte da Anatel ocorrem de maneira fundamentada para atendimento às atividades de fiscalização demandadas pelas áreas internas da Agência, como as áreas de acompanhamento e controle de obrigações, para estudos setoriais, respostas a entes externos como Poder Judiciário, TCU, CGU, Ministério Público, Poder Legislativo, entre outros. Em todos os casos, as solicitações apresentadas às prestadoras são feitas com base em justificativas associadas a motivações específicas.<br>Qualquer fiscalização efetuada via acesso remoto (ou on-line) é devidamente fundamentada e o acesso é realizado mediante prévia solicitação/comunicação da Anatel, o que permite acompanhamento da prestadora fiscalizada.<br>Nos exatos termos do art. 27, § 3º, da Resolução nº 596, de 6 de agosto de 2012, que aprovou o Regulamento de Fiscalização da Anatel, "no caso de acesso on-line serão sempre assegurados à fiscalizada o conhecimento simultâneo da realização do procedimento e a rastreabilidade dos dados e informações acessados pela Anatel."<br>Ademais, cabe ressaltar que além de todas as prerrogativas e obrigações legais dos agentes de fiscalização (servidores públicos federais), para acesso remoto (ou on-line) a sistemas das prestadoras, a Anatel realiza um procedimento de credenciamento específico para os agentes que farão uso de tal sistemática, conforme disciplinamento estabelecido na Portaria Anatel no 942, de 29 de novembro de 2013, que aprova orientações específicas para implementação do modo de acesso on-line em atividades de fiscalização.<br><br>5) Por que meio se dá o compartilhamento e o acesso aos dados? Há utilização de software? Se sim, qual?<br>O compartilhamento e o acesso aos dados podem ocorrer de diversas formas: envio em meios físicos como DVDs e discos rígidos, por meio de acesso remoto ftp para dowload de arquivos de dados, por meio de acesso direto às telas dos sistemas das operadoras (via conexões VPN que observam todas as prerrogativas de segurança da informação implementadas pelas áreas de TI das prestadoras), por meio de cadastro pelas próprias operadoras das informações solicitadas nos sistemas de informação da Anatel tais como o SICI - Sistema de Coleta de Informações, SGMU – Sistema de Gestão de Metas de Universalização, entre outros, listados na página da Anatel no endereço: http://www.anatel.gov.br/institucional/sistemas-interativos. |
| Responsável pela Resposta | Gerência de Fiscalização (FIGF) |
| Destinatário do Recurso de Primeira Instância: | Superintendência de Fiscalização (SFI) |
| Prazo Limite para Recurso | 16/02/2017 |
| *Classificação do Pedido* | |

| | |
|---|---|
| Categoria do Pedido | Ciência, Informação e Comunicação |
| Subcategoria do Pedido | Informação - Gestão, preservação e acesso |
| Número de Perguntas | 5 |

**Histórico do Pedido**

| Data do evento | Descrição do evento | Responsável |
|---|---|---|
| 17/01/2017 12:05 | Pedido Registrado para o Órgão ANATEL – Agência Nacional de Telecomunicações | SOLICITANTE |
| 06/02/2017 15:24 | Pedido Respondido | MC – Ministério das Comunicações/ANATEL – Agência Nacional de Telecomunicações |

# 4.2. ANEXO II



**RELATÓRIO DE QUANTITATIVOS**

**Esfera:** .:TODOS(AS):.
**Ano:** SELECIONE
**Mês:** SELECIONE
**Tipo de Relatório:** TABELA

Gerar relatório

***LEGENDA**

**Total 1** = Quantidade de Ofícios Expedidos (inicial)

**Total 2** = Quantidade de Ofícios Expedidos (total em andamento)

**Total 3** = Quantidade de Procedimentos Criminais Instaurados (inicial)

**Total 4** = Quantidade de Procedimentos Criminais Instaurados (total em andamento)

**Total 5** = Quantidade de Telefones Monitorados (total em andamento)

**Total 6** = Quantidade de Telefones Monitorados - VOIP (total em andamento)

**Total 7** = Quantidade de Ofícios Expedidos (inicial)

**Total 8** = Quantidade de Ofícios Expedidos (total em andamento)

**Total 9** = Quantidade de Procedimentos Criminais Instaurados (inicial)

**Total 10** = Quantidade de Procedimentos Criminais Instaurados (total em andamento)

**Total 11** = Quantidade de Endereços Eletrônicos Monitorados (total em andamento)

| Mês/Ano | Total 1 | Total 2 | Total 3 | Total 4 | Total 5 | Total 6 | Total 7 | Total 8 | Total 9 | Total 10 | Total 11 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 0/0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Janeiro/2008 | 19 | 20 | 5 | 8 | 32 | 0 | 0 | 0 | 0 | 1 | 0 |
| Fevereiro/2008 | 39 | 122 | 12 | 17 | 170 | 7 | 0 | 0 | 0 | 0 | 0 |
| Março/2008 | 33 | 54 | 7 | 14 | 58 | 0 | 1 | 1 | 0 | 0 | 1 |
| Abril/2008 | 51 | 113 | 15 | 18 | 99 | 28 | 1 | 1 | 2 | 2 | 1 |
| Maio/2008 | 25 | 54 | 9 | 11 | 80 | 4 | 0 | 0 | 0 | 0 | 0 |
| Junho/2008 | 76 | 87 | 22 | 34 | 119 | 8 | 0 | 0 | 0 | 0 | 0 |
| Julho/2008 | 80 | 95 | 26 | 32 | 184 | 25 | 1 | 1 | 1 | 1 | 1 |
| Agosto/2008 | 69 | 90 | 23 | 52 | 234 | 9 | 0 | 0 | 0 | 0 | 0 |
| Setembro/2008 | 296 | 531 | 56 | 120 | 1067 | 23 | 24 | 36 | 5 | 13 | 39 |
| Outubro/2008 | 517 | 930 | 143 | 238 | 1511 | 207 | 31 | 38 | 3 | 11 | 22 |
| Novembro/2008 | 1133 | 2247 | 255 | 624 | 5559 | 276 | 41 | 68 | 25 | 54 | 14 |
| Dezembro/2008 | 1470 | 2926 | 408 | 2274 | 7476 | 240 | 119 | 186 | 39 | 229 | 22 |
| Janeiro/2009 | 2119 | 4085 | 496 | 1313 | 8421 | 742 | 109 | 187 | 74 | 157 | 119 |
| Fevereiro/2009 | 2434 | 4830 | 539 | 1528 | 9549 | 762 | 75 | 133 | 53 | 177 | 412 |
| Março/2009 | 3377 | 6054 | 754 | 1912 | 11210 | 808 | 139 | 234 | 70 | 259 | 252 |
| Abril/2009 | 3092 | 6030 | 653 | 1917 | 11462 | 886 | 105 | 298 | 76 | 255 | 242 |
| Maio/2009 | 3170 | 6047 | 676 | 2057 | 12091 | 738 | 111 | 242 | 69 | 258 | 380 |
| Junho/2009 | 3417 | 6676 | 729 | 2013 | 12369 | 760 | 245 | 391 | 102 | 330 | 345 |
| Julho/2009 | 3942 | 7598 | 871 | 2528 | 13991 | 881 | 163 | 362 | 98 | 324 | 287 |
| Agosto/2009 | 3675 | 7697 | 847 | 2694 | 13472 | 825 | 190 | 435 | 89 | 347 | 375 |
| Setembro/2009 | 3861 | 7471 | 956 | 2821 | 14939 | 931 | 191 | 492 | 161 | 476 | 481 |
| Outubro/2009 | 4202 | 7955 | 943 | 2848 | 15463 | 1368 | 183 | 501 | 108 | 402 | 347 |
| Novembro/2009 | 3561 | 7583 | 870 | 2884 | 14698 | 1226 | 201 | 526 | 118 | 432 | 314 |
| Dezembro/2009 | 2795 | 6633 | 679 | 2598 | 12138 | 1017 | 154 | 512 | 63 | 423 | 330 |
| Janeiro/2010 | 3121 | 6804 | 788 | 2685 | 12194 | 1075 | 212 | 654 | 106 | 441 | 347 |
| Fevereiro/2010 | 3689 | 7952 | 814 | 2795 | 15080 | 1160 | 207 | 436 | 86 | 403 | 268 |
| Março/2010 | 5238 | 10052 | 1201 | 3356 | 18796 | 1076 | 240 | 401 | 158 | 500 | 256 |
| Abril/2010 | 4771 | 9732 | 1016 | 3330 | 18269 | 1124 | 199 | 379 | 138 | 481 | 429 |
| Maio/2010 | 5142 | 10442 | 1089 | 3496 | 18929 | 1476 | 199 | 417 | 187 | 497 | 298 |
| Junho/2010 | 4696 | 9633 | 1028 | 3635 | 17880 | 1339 | 157 | 389 | 112 | 689 | 355 |
| Julho/2010 | 5029 | 10236 | 1141 | 3650 | 18969 | 1332 | 173 | 388 | 107 | 422 | 346 |
| Agosto/2010 | 5018 | 10226 | 1163 | 3669 | 18354 | 1316 | 229 | 458 | 119 | 424 | 431 |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Setembro/2010 | 4709 | 10651 | 1171 | 3575 | 20653 | 1687 | 168 | 411 | 82 | 288 | 949 |
| Outubro/2010 | 4484 | 10605 | 1103 | 3659 | 21515 | 1537 | 192 | 462 | 77 | 269 | 354 |
| Novembro/2010 | 4360 | 9503 | 1145 | 3476 | 18958 | 1399 | 211 | 393 | 78 | 258 | 411 |
| Dezembro/2010 | 3125 | 7622 | 812 | 3027 | 15286 | 656 | 132 | 294 | 43 | 166 | 288 |
| Janeiro/2011 | 3221 | 8013 | 798 | 3184 | 15519 | 749 | 122 | 279 | 45 | 191 | 276 |
| Fevereiro/2011 | 4293 | 9026 | 1091 | 3410 | 17810 | 946 | 183 | 349 | 62 | 207 | 253 |
| Março/2011 | 4691 | 10282 | 1148 | 3584 | 20059 | 1018 | 173 | 317 | 62 | 185 | 287 |
| Abril/2011 | 4735 | 10498 | 1136 | 3684 | 19765 | 1036 | 251 | 373 | 87 | 209 | 391 |
| Maio/2011 | 4946 | 11236 | 1149 | 3824 | 19885 | 1596 | 233 | 386 | 110 | 244 | 389 |
| Junho/2011 | 4907 | 11519 | 1143 | 4165 | 21339 | 1609 | 229 | 409 | 96 | 256 | 411 |
| Julho/2011 | 4779 | 11237 | 1017 | 3652 | 20008 | 1403 | 235 | 417 | 90 | 257 | 374 |
| Agosto/2011 | 5259 | 11923 | 1156 | 3916 | 21589 | 1044 | 205 | 371 | 85 | 269 | 348 |
| Setembro/2011 | 5340 | 12377 | 1179 | 3974 | 21887 | 1626 | 171 | 352 | 83 | 348 | 413 |
| Outubro/2011 | 4364 | 11311 | 1013 | 3719 | 19921 | 972 | 173 | 336 | 79 | 306 | 229 |
| Novembro/2011 | 4391 | 11013 | 1015 | 3832 | 18724 | 1301 | 169 | 297 | 55 | 292 | 284 |
| Dezembro/2011 | 3239 | 9162 | 770 | 3497 | 16548 | 1231 | 166 | 366 | 68 | 324 | 356 |
| Janeiro/2012 | 3699 | 9193 | 1009 | 3804 | 17289 | 1120 | 146 | 283 | 53 | 265 | 281 |
| Fevereiro/2012 | 3849 | 9633 | 966 | 3680 | 18239 | 1276 | 184 | 344 | 65 | 271 | 267 |
| Março/2012 | 4852 | 11171 | 1127 | 3921 | 22499 | 1432 | 208 | 377 | 68 | 306 | 349 |
| Abril/2012 | 4869 | 11515 | 1171 | 3847 | 22252 | 1307 | 177 | 439 | 63 | 301 | 377 |
| Maio/2012 | 5156 | 12169 | 1247 | 4084 | 24964 | 1725 | 163 | 328 | 86 | 323 | 523 |
| Junho/2012 | 4510 | 11708 | 1100 | 3909 | 23652 | 1612 | 175 | 336 | 79 | 309 | 436 |
| Julho/2012 | 4658 | 11783 | 1126 | 3966 | 23242 | 1897 | 179 | 410 | 65 | 375 | 508 |
| Agosto/2012 | 4701 | 11838 | 1183 | 4393 | 23268 | 1587 | 148 | 449 | 49 | 362 | 513 |
| Setembro/2012 | 4257 | 10601 | 1107 | 4272 | 18243 | 1842 | 135 | 390 | 80 | 336 | 310 |
| Outubro/2012 | 4438 | 11134 | 1125 | 4157 | 19595 | 2074 | 199 | 509 | 54 | 315 | 489 |
| Novembro/2012 | 4053 | 10742 | 1061 | 3918 | 19206 | 1920 | 137 | 403 | 48 | 244 | 396 |
| Dezembro/2012 | 2754 | 9032 | 721 | 3617 | 15168 | 1792 | 117 | 349 | 63 | 269 | 295 |
| Janeiro/2013 | 3428 | 9383 | 973 | 3757 | 16295 | 1888 | 167 | 440 | 89 | 275 | 347 |
| Fevereiro/2013 | 3333 | 9068 | 901 | 3527 | 17289 | 1890 | 90 | 191 | 67 | 237 | 316 |
| Março/2013 | 4204 | 10358 | 1054 | 3922 | 18832 | 2230 | 121 | 269 | 83 | 278 | 731 |
| Abril/2013 | 4992 | 11079 | 1206 | 4297 | 22401 | 2211 | 253 | 486 | 82 | 312 | 911 |
| Maio/2013 | 4360 | 9931 | 1114 | 4588 | 20721 | 2297 | 160 | 299 | 88 | 350 | 815 |
| Junho/2013 | 4206 | 9392 | 1077 | 4340 | 20985 | 2445 | 346 | 795 | 96 | 396 | 1146 |
| Julho/2013 | 4438 | 10529 | 1115 | 4440 | 23378 | 2319 | 217 | 362 | 80 | 332 | 921 |
| Agosto/2013 | 4598 | 9543 | 1134 | 4456 | 21925 | 2404 | 207 | 399 | 97 | 333 | 1563 |
| Setembro/2013 | 4032 | 9046 | 1036 | 4376 | 22473 | 2599 | 225 | 382 | 85 | 274 | 1090 |
| Outubro/2013 | 4049 | 9511 | 1029 | 4256 | 21242 | 1622 | 180 | 355 | 65 | 199 | 1605 |
| Novembro/2013 | 3762 | 8508 | 1018 | 3951 | 20877 | 2784 | 191 | 317 | 61 | 239 | 1470 |
| Dezembro/2013 | 2579 | 6664 | 712 | 3550 | 16035 | 1435 | 151 | 288 | 54 | 243 | 1063 |
| Janeiro/2014 | 3019 | 6903 | 824 | 3594 | 16653 | 1812 | 119 | 310 | 57 | 218 | 1100 |
| Fevereiro/2014 | 3755 | 7633 | 1026 | 3805 | 19724 | 2206 | 160 | 358 | 56 | 236 | 1084 |
| Março/2014 | 3814 | 7964 | 982 | 3905 | 19485 | 2404 | 178 | 454 | 72 | 272 | 1110 |
| Abril/2014 | 3883 | 8345 | 1031 | 4100 | 20651 | 2345 | 272 | 379 | 85 | 292 | 1190 |
| Maio/2014 | 4327 | 8876 | 1093 | 3981 | 19752 | 2262 | 253 | 418 | 89 | 345 | 996 |
| Junho/2014 | 4006 | 8583 | 1019 | 4274 | 18717 | 2261 | 205 | 495 | 156 | 412 | 1195 |
| Julho/2014 | 4465 | 9484 | 1118 | 4494 | 21438 | 2321 | 273 | 485 | 90 | 377 | 1443 |
| Agosto/2014 | 4160 | 9040 | 1047 | 4037 | 22714 | 2016 | 204 | 379 | 101 | 324 | 1365 |
| Setembro/2014 | 4192 | 9045 | 1093 | 4220 | 21030 | 2261 | 242 | 432 | 130 | 446 | 1409 |
| Outubro/2014 | 4127 | 8828 | 1084 | 4219 | 21200 | 2383 | 213 | 400 | 125 | 429 | 1488 |
| Novembro/2014 | 3457 | 7994 | 865 | 3986 | 21625 | 1864 | 160 | 308 | 76 | 396 | 1302 |
| Dezembro/2014 | 2436 | 6388 | 682 | 3635 | 17634 | 1880 | 156 | 273 | 88 | 389 | 1125 |
| Janeiro/2015 | 2738 | 6165 | 730 | 3523 | 17758 | 1544 | 154 | 276 | 102 | 578 | 1007 |
| Fevereiro/2015 | 3191 | 7107 | 900 | 3786 | 19642 | 1684 | 207 | 353 | 84 | 520 | 1400 |
| Março/2015 | 4342 | 8583 | 1083 | 4069 | 22268 | 2272 | 250 | 442 | 131 | 558 | 1450 |
| Abril/2015 | 3951 | 8423 | 987 | 4122 | 23804 | 2226 | 278 | 454 | 112 | 546 | 1722 |
| Maio/2015 | 4155 | 8753 | 1109 | 4525 | 24224 | 2178 | 275 | 440 | 114 | 597 | 1605 |
| Junho/2015 | 3839 | 8613 | 935 | 4086 | 25571 | 2224 | 225 | 458 | 94 | 603 | 1510 |
| Julho/2015 | 4071 | 8854 | 945 | 4337 | 24571 | 1978 | 205 | 380 | 129 | 597 | 1617 |
| Agosto/2015 | 3713 | 8849 | 1023 | 4598 | 24991 | 1950 | 214 | 388 | 130 | 616 | 1762 |
| Setembro/2015 | 3474 | 8289 | 959 | 4183 | 23668 | 1820 | 228 | 449 | 103 | 574 | 1527 |
| Outubro/2015 | 3489 | 8197 | 1014 | 4237 | 23809 | 1694 | 248 | 496 | 133 | 591 | 1644 |
| Novembro/2015 | 3082 | 7458 | 925 | 4351 | 21683 | 1811 | 261 | 573 | 114 | 580 | 1684 |
| Dezembro/2015 | 2630 | 6190 | 693 | 3890 | 19375 | 1472 | 193 | 299 | 87 | 523 | 1245 |
| Janeiro/2016 | 2555 | 6128 | 865 | 3776 | 18173 | 1111 | 184 | 318 | 86 | 495 | 1377 |
| Fevereiro/2016 | 3091 | 7039 | 852 | 3626 | 19489 | 1709 | 207 | 395 | 103 | 245 | 977 |
| Março/2016 | 3552 | 7768 | 1004 | 3685 | 21113 | 1414 | 224 | 484 | 107 | 279 | 941 |
| Abril/2016 | 3626 | 8070 | 972 | 3789 | 22088 | 1427 | 232 | 526 | 138 | 324 | 1068 |
| Maio/2016 | 3642 | 8280 | 922 | 3811 | 23175 | 1276 | 213 | 497 | 128 | 328 | 917 |
| Junho/2016 | 3538 | 8296 | 1042 | 3999 | 25123 | 1570 | 225 | 468 | 118 | 327 | 1089 |
| Julho/2016 | 3390 | 7972 | 940 | 3763 | 21302 | 1480 | 256 | 476 | 107 | 314 | 661 |
| Agosto/2016 | 3542 | 7859 | 885 | 3690 | 21927 | 1835 | 226 | 456 | 103 | 312 | 845 |
| Setembro/2016 | 3138 | 7336 | 854 | 3702 | 20915 | 1734 | 296 | 500 | 110 | 331 | 899 |
| Outubro/2016 | 3421 | 8024 | 912 | 3765 | 21105 | 2021 | 218 | 373 | 118 | 390 | 1032 |
| Novembro/2016 | 2759 | 6915 | 800 | 3435 | 20958 | 1512 | 254 | 398 | 153 | 338 | 723 |
| Dezembro/2016 | 2050 | 6077 | 550 | 3170 | 19677 | 1209 | 156 | 328 | 93 | 321 | 537 |
| Janeiro/2017 | 2208 | 6313 | 643 | 3050 | 19753 | 1101 | 222 | 451 | 71 | 271 | 540 |
| Fevereiro/2017 | 2692 | 6292 | 777 | 3249 | 22371 | 1353 | 280 | 449 | 102 | 297 | 970 |
| Março/2017 | 3062 | 6680 | 810 | 2895 | 24931 | 1374 | 198 | 387 | 115 | 291 | 791 |
| Abril/2017 | 938 | 1931 | 216 | 873 | 6676 | 363 | 51 | 109 | 19 | 80 | 506 |
| Maio/2017 | 20 | 24 | 7 | 18 | 72 | 2 | 0 | 0 | 4 | 4 | 0 |
| **Total** | **386307** | **876082** | **96610** | **364630** | **1945234** | **158546** | **19604** | **39492** | **9224** | **35187** | **76302** |

## 4.3. ANEXO III

SERVIÇO PÚBLICO FEDERAL
MJ - POLÍCIA FEDERAL
DIREÇÃO GERAL

# Mensagem Eletrônica n° 084/2016 - GAB/PF

| | DADOS DO RECURSO |
|---|---|
| Protocolo | 08850003036201611 |
| Solicitante | J.P.V.S. |
| Data de abertura (pedido) | 27/09/2016 |
| Órgão Superior Destinatário | MJC – Ministério da Justiça e Cidadania |
| Órgão Vinculado Destinatário | Polícia Federal |
| Prazo para atendimento (recurso) | 17/10/2016 |
| Forma de recebimento da resposta | Pelo sistema (com avisos por e-mail) |

**1.** Trata-se de recurso interposto por J.P.V.S. nos autos do pedido de acesso à informação registrado no sistema e-SIC sob o NUP 08850003036201611.

**2.** O requerente registrou pedido de acesso nos seguintes termos:

*"Gostaria de fazer algumas perguntas sobre a utilização de softwares de monitoramento pela Polícia Federal.*
*1) A Polícia Federal emprega softwares de monitoramento de computadores e/ou dispositivos móveis em suspeitos investigados?*
*2) Que tipo de autorização judicial os agentes precisam para utilizar softwares deste tipo?*
*3) Qual ou quais softwares são utilizados em operações do tipo?*
*4) Ao todo, quantas pessoas foram monitoradas por meio de softwares de monitoramento em 2016?."*

**3.** Em resposta, o SIC/DIP/PF informou o que segue:

*"Senhor Requerente,*
*1)De acordo com a Mensagem Circular nº 01 e 02 de 2014, CIDIC 09004.000277/2014-18 S.05.10/04/2014.09/04/2029.N. Estão preservadas do acesso público as informações relacionadas à capacidade técnica dos sistema de interceptação de sinais contratados pela Polícia Federal. Funções e recursos disponíveis, quantidade de canais, capacidades de usuários, capacidade de números interceptáveis, tecnologias compatíveis, localização*

*física dos equipamentos, requisitos técnicos para instalação e funcionamentos, facilidades dos sistemas, forma de gerenciamento, capacidade de armazenamento, diagramas técnicos, sistemas de emergência, meios de transmissão de dados, unidades que utilizam os sistemas, dentre outras de natureza similar.*

*Além disso, também são classificados os dados de caráter técnico operacional ou estratégico intrínsecas às atividades da Polícia Federal, tais como qualidade e distribuição de efetivo, infraestrutura, modo de atuação, comunicações, sistemas, entre outras de natureza similar.*

*2) A interceptação de sinais deve se realizar com autorização judicial, de acordo com a Lei nº 9.296/96.*

*3) São classificados os dados de caráter técnico operacional ou estratégico intrínsecas às atividades da Polícia Federal, tais como qualidade e distribuição de efetivo, infraestrutura, modo de atuação, comunicações, sistemas, entre outras de natureza similar.*

*4) Também são classificados os dados de caráter técnico operacional ou estratégico intrínsecas às atividades da Polícia Federal, tais como qualidade e distribuição de efetivo, infraestrutura, modo de atuação, comunicações, sistemas, entre outras de natureza similar..”*

**4.** Insatisfeito, o requerente interpôs recurso de 1ª instância ao DG/PF, sob os seguintes argumentos:

*“Olá, tudo bem?*

*1 - Em relação à minha primeira pergunta, ainda que as capacidades técnicas e especificidades de uso estejam protegidas por sigilo, a minha pergunta é objetivo no que tange ao conhecimento do uso de softwares de monitoramento possivelmente utilizados pela PF. Mesmo que sem detalhes, é possível sanar essa questão, ou seja, esclarecer se SIM ou NÃO, a Polícia Federal tem acesso à programas capazes de acessar celulares, dispositivos móveis e computadores de suspeitos em potencial?*

*2 - Segundo alguns especialistas consultados, a Lei nº 9.296/96 diz respeito apenas à interceptação de informações em trânsito (como uma chamada telefônica ou carta). Caso o monitoramento seja feito de maneira direta no computador, por exemplo, de um suspeito, esse arcabouço jurídico não seria o suficiente para fornecer autorização. Ainda assim, esse é o tipo de autorização que a PF busca quando (e SE) faz operações do tipo?*

*3 - Ok.*

*4 - Ok..”.*

**5.** Verifica-se que o requerente teve sua pretensão parcialmente satisfeita e que suas razões de recorrer incidem apenas sobre os itens 1 e 2 do pedido inicial.

**6.** **Em relação ao quesito 1:**

**7.** A capacidade técnica dos sistemas de interceptação de sinais contratados pela Polícia Federal estão protegidos do acesso público por meio do Termo de Classificação CIDIC 09004.000277/2014-18 S.05.10/04/2014.09/04/2029.N.

**8.** A mera resposta dual ("sim" ou não") fornece ao cidadão peticionário dados sobre a capacidade investigatória da Polícia Federal, pois acaba por identificar dados de caráter técnico operacional ou estratégico intrínsecos às atividades da Polícia Federal, sob restrição de sigilo.

**9.** Não bastasse isso, dispõe a Lei n.º 12.850 em seu art. 3º, §1.º: "Havendo necessidade justificada de manter sigilo sobre a capacidade investigatória, poderá ser dispensada licitação para contratação de serviços técnicos especializados, aquisição ou locação de equipamentos destinados à polícia judiciária para o rastreamento e obtenção de provas previstas nos incisos II e V. (Incluído pela Lei nº 13.097, de 2015)".

**10.** A licitação destina-se não apenas a garantir a observância do princípio da publicidade, mas também da legalidade, da impessoalidade, da moralidade, da igualdade, da probidade administrativa, da vinculação ao instrumento convocatório, do julgamento objetivo, bem como para garantir a observância do princípio constitucional da isonomia, a seleção da proposta mais vantajosa para a administração e a promoção do desenvolvimento nacional sustentável.

**11.** Assim, se a norma acima mencionada permite a dispensa de licitação justamente com o intuito de preservação do sigilo da capacidade investigatória, em uma interpretação teleológica há de se entender que foi criado nova modalidade de sigilo, por meio de lei ordinária posterior à Lei de Acesso à Informação, em relação a tal informação.

**12.** Referido sigilo encontra-se devidamente amparado pelo art. 5.º, caput, da Constituição Federal e por seu inciso XXXIII, que dispõem:

> *Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: (...)*

> *XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado; (...)*

**13.** Afinal de nada adiantaria a excepcionalização do processo de licitação se, por vias transversas, terceiros pudessem ter acesso à informações sobre a capacidade investigatória da instituição.

**14.** Ressaltamos que a Lei de Acesso à Informação foi extremamente bem vinda em nosso ordenamento jurídico, pois regulamentou importante mecanismo de participação popular direta no controle das ações governamentais. Contudo, dita lei não criou direto absoluto ao acesso a informações, pois além de exceções previstas em seu próprio texto, dispôs em seu art. 22 que ***"o disposto nesta Lei não exclui as demais hipóteses legais de sigilo e de segredo de justiça nem as hipóteses de segredo industrial decorrentes da exploração direta de atividade econômica pelo Estado ou por pessoa física ou entidade privada que tenha qualquer vínculo com o poder público".***

**15.** Assim, claramente ficaram excepcionadas do alcance da norma quaisquer outras situações previstas em lei e acobertadas por sigilo, tal qual se verifica no caso em comento. Neste caso, o nosso ordenamento jurídico afasta a regra da publicidade com o intuito de preservar-se o **direito fundamental a segurança**.

**16.** **Em relação ao quesito 2:**

**17.** O quesito 2 versa sobre os procedimentos judiciais adotados pela Polícia Federal em suas investigações.

**18.** A resposta inicial dada pelo SIC/DIP/PF deu-se satisfatoriamente, haja vista ter informado que as autorizações judiciais são tomadas com base na Lei n. 9.296/96. A irresignação do cidadão não se deu pela negativa do órgão em responder ao seu questionamento, mas sim com relação ao mérito da resposta em si.

**19.** Em casos como esse, não é possível conhecer do recurso, uma vez que não houve negativa da Polícia Federal em fornecer as informações.

**20.** As razões recursais limitam-se a questionar o porquê da Polícia Federal amparar-se na Lei n. 9.296/96.

**21.** Com a devida vênia, não há como acolher a pretensão recursal porque o pedido de acesso teve o adequado tratamento no âmbito da DIP/PF, que respondeu ao item de forma clara, objetiva e precisa.

**22.** Nesses termos, satisfeita totalmente a pretensão de acesso por meio da resposta ao pedido original, não há que se falar em pretensão recursal.

**23.** Nesses termos, diante dos argumentos acima expendidos, **conheço** e **nego provimento** ao recurso, com relação ao item 1, e **não conheço** do recurso com relação ao item 2.

**24.** Informo, ainda, que a requerente tem direito a recurso ao Exmo. Sr. Ministro da Justiça e Cidadania, no prazo de 10 (dez) dias, contados da ciência da resposta, que pode ser apresentado via sistema e-SIC - www.acessoainformacao.gov.br/sistema.

Brasília, 17 de outubro de 2016.

Leandro Daiello Coimbra
Diretor-Geral
PF/MJC

3155682 08850003036201611

**MINISTÉRIO DA JUSTIÇA E CIDADANIA**

# DESPACHO DO MINISTRO

Em 25 de outubro de 2016

Pedido SIC nº 08850.003036/2016-11
Interessado/Recorrente: João Paulo Vicente da Silveira
Órgão Recorrido: Departamento de Polícia Federal
Assunto: Recurso em segunda instância impetrado contra decisão do Departamento de Polícia Federal

Considerando a Lei nº 12.527, de 2011, e o Decreto nº 7.724, de 2012, acolho os argumentos apresentados pela Informação n° 77/2016/STAI/OUVG/GM (3153596), de 21 de outubro de 2016, para **conhecer e negar provimento** quanto ao item **I** e **não conhecer do recurso** no tocante ao item **II** do recurso em segunda instância interposto pelo cidadão João Paulo Vicente da Silveira em face da decisão do Departamento de Polícia Federal.

Dê-se ciência ao recorrente e ao órgão recorrido.

ALEXANDRE DE MORAES
Ministro de Estado da Justiça e Cidadania

Documento assinado eletronicamente por **ALEXANDRE DE MORAES**, **Ministro de Estado da Justiça e Cidadania**, em 25/10/2016, às 14:52, conforme o § 2º do art. 10 da Medida Provisória nº 2.200/01.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **3155682** e o código CRC **82C35AEC**
O trâmite deste documento pode ser acompanhado pelo site http://www.justica.gov.br/acesso-a-sistemas/protocolo e tem validade de prova de registro de protocolo no Ministério da Justiça.

**Referência:** Processo nº 08850003036201611 SEI nº 3155682

3153596 08850003036201611

**MINISTÉRIO DA JUSTIÇA E CIDADANIA**

**INFORMAÇÃO Nº 77/2016/STAI/OUVG/GM**

**Processo nº 08850003036201611**

**Recorrente: João Paulo Vicente da Silveira**

**Órgão/entidade recorrida:** DPF - Departamento de Polícia Federal

I. ANÁLISE DE ADMISSIBILIDADE DO RECURSO

O recurso foi interposto dentro do prazo legal de 10 dias da ciência da decisão, sendo, dessa forma, tempestivo. O recorrente utilizou-se do recurso conferido pelo Art. 21, parágrafo único do Decreto nº 7.724/2012, não havendo supressão de instância. O interessado é legitimado para recorrer nos termos do inciso III, do art. 63, da Lei nº 9.784/1999.

II. ANÁLISE DO MÉRITO

O recorrente requer informações sobre a utilização de softwares de monitoramento pela Polícia Federal, e faz os seguintes questionamentos: **I** - A Polícia Federal emprega softwares de monitoramento de computadores e/ou dispositivos móveis em suspeitos investigados? **II** - Que tipo de autorização judicial os agentes precisam para utilizar softwares desse tipo? **III** - Qual ou quais softwares são utilizados em operações deste tipo? **IV** - Ao todo, quantas pessoas foram monitoradas por meio de softwares de monitoramento em 2016?

Após análise do pleito, verificou-se que o questionamento número **I** do recorrente não poderá ser atendido, tendo em vista se tratar de informação classificada sob número de **CIDIC 09004.000277/2014-18 S.05.10/04/2014.09/04/2029.N.** Portanto, qualquer afirmativa ou negativa referente a informação solicitada, violaria o sigilo do documento, principalmente pelo fato de ser informação ligada a investigação policial.

Quanto ao item **II** do presente pedido de acesso, entende-se tratar-se de demanda fora do escopo da Lei de Acesso à Informação - Lei nº 12.527/2011, uma vez que solicita interpretação de normas e procedimentos por parte da administração pública.

No tocante aos questionamentos **III** e **IV** do pedido em tela, cumpre destacar que tratam-se de informações classificadas sob o número de Código de Indexação Classificada - CIDIC **0800.000277/2014-18.S.05.10/04/2014.09/04/2029.N**. Contudo, em complemento à resposta da recorrida, seguirá apenso a este documento, cópia do referido TCI com suas razões de classificação devidamente obliteradas, conforme preconiza o parágrafo 2º do Art. 31 do Decreto 7.724/2012.

Assim, sugere-se **conhecer e negar provimento** quanto ao item **I**, devido à restrição de acesso à informações classificadas, e **não conhecer do recurso** no tocante ao item **II**, tendo em vista não se tratar de pedido de acesso à informação.

---

Documento assinado eletronicamente por **LUCAS CHAVES FERNANDES**, **Ouvidor(a)-Geral do Ministério da Justiça - Substituto(a)**, em 21/10/2016, às 17:36, conforme o § 2º do art. 10 da Medida Provisória nº 2.200/01.

Documento assinado eletronicamente por **MOISÉS PAES LANDIN PLÁCIDO**, **Chefe do Serviço de Transparência e Acesso à Informação**, em 21/10/2016, às 19:36, conforme o § 2º do art. 10 da Medida Provisória nº 2.200/01.

A autenticidade do documento pode ser conferida no site http://sei.autentica.mj.gov.br informando o código verificador **3153596** e o código CRC **9A469614**
O trâmite deste documento pode ser acompanhado pelo site http://www.justica.gov.br/acesso-a-sistemas/protocolo e tem validade de prova de registro de protocolo no Ministério da Justiça.

**Referência:** Processo nº 08850003036201611 SEI nº 3153596

**GRAU DE SIGILO: SECRETO**

| TERMO DE CLASSIFICAÇÃO DE INFORMAÇÃO | |
|---|---|
| ÓRGÃO/ENTIDADE: Departamento de Polícia Federal (DPF) | |
| CÓDIGO DE INDEXAÇÃO: 08004.000277/2014-18.S.05.10/04/2014.09/04/2029.N | |
| GRAU DE SIGILO: Secreto | |
| CATEGORIA: 05 | |
| TIPO DE DOCUMENTO: Nota Técnica | |
| DATA DE PRODUÇÃO: 29/04/2014 | |
| FUNDAMENTO LEGAL PARA CLASSIFICAÇÃO: Art. 23, III e VIII, da Lei nº 12.527/2011 | |
| RAZÕES PARA A CLASSIFICAÇÃO: [redacted] | |
| PRAZO DA RESTRIÇÃO DE ACESSO: 15 anos | |
| DATA DE CLASSIFICAÇÃO: 29/04/2014 | |
| AUTORIDADE CLASSIFICADORA | Nome: José Eduardo Cardozo<br>Cargo: Ministro de Estado da Justiça |
| AUTORIDADE RATIFICADORA (quando aplicável) | Nome:<br>Cargo: |
| DESCLASSIFICAÇÃO em ___/___/_____ (quando aplicável) | Nome:<br>Cargo: |
| RECLASSIFICAÇÃO em ___/___/_____ (quando aplicável) | Nome:<br>Cargo: |
| REDUÇÃO DE PRAZO em ___/___/_____ (quando aplicável) | Nome:<br>Cargo: |
| PRORROGAÇÃO DE PRAZO em ___/___/_____ (quando aplicável) | Nome:<br>Cargo: |

ASSINATURA DA AUTORIDADE CLASSIFICADORA

ASSINATURA DA AUTORIDADE RATIFICADORA (quando aplicável)

ASSINATURA DA AUTORIDADE responsável por DESCLASSIFICAÇÃO (quando aplicável)

ASSINATURA DA AUTORIDADE responsável por RECLASSIFICAÇÃO (quando aplicável)

ASSINATURA DA AUTORIDADE responsável por REDUÇÃO DE PRAZO (quando aplicável)

ASSINATURA DA AUTORIDADE responsável por PRORROGAÇÃO DE PRAZO (quando aplicável)

INTERNETLAB


Equipe do Projeto

Diretor

Dennys Antonialli

Pesquisadora

Jacqueline de Souza Abreu

Equipe Institucional

Diretor

Dennys Antonialli

Diretor

Francisco Brito Cruz

Diretora

Mariana Giorgetti Valente

InternetLab.org.br

Av Ipiranga 344 cj 11B

São Paulo SP