

# VIGILÂNCIA DAS COMUNICAÇÕES PELO ESTADO BRASILEIRO

## E A PROTEÇÃO A DIREITOS FUNDAMENTAIS



ELECTRONIC FRONTIER FOUNDATION

INTERNETLAB

pesquisa em direito e tecnologia

# VIGILÂNCIA DAS COMUNICAÇÕES PELO ESTADO BRASILEIRO

## ***Autores:***

Dennys Antonialli

Jacqueline de Souza Abreu



**Relatório elaborado em parceria com a Electronic Frontier Foundation (EFF)**

**Contribuíram**

*Artigo 19*

*Oficina Antivigilância*

Este relatório é parte do projeto “Vigilância e Direitos Humanos” realizado em oito países da América Latina pela Electronic Frontier Foundation, uma organização internacional sem fins lucrativos que, desde 1990, defende a liberdade de expressão e a privacidade na era digital.



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.

Este trabalho está licenciado sob uma licença Creative Commons CC BY 3.0 BR. Essa licença permite que outros remixem, adaptem e criem obras derivadas sobre a obra original, inclusive para fins comerciais, contanto que atribuam crédito ao autor corretamente.

Texto da licença:

<https://creativecommons.org/licenses/by/3.0/br/legalcode>

\*\*\*

## **EQUIPE INSTITUCIONAL:**

*Diretor Presidente:* Dennys Antonialli; *Diretor:* Francisco Brito Cruz; *Diretora:* Mariana Giorgetti Valente.

ASSOCIAÇÃO INTERNETLAB DE PESQUISA EM DIREITO E TECNOLOGIA, 2015.

INTERNETLAB / Rua Augusta, 2690, Galeria Ouro Fino, Loja 326 / [www.internetlab.org.br](http://www.internetlab.org.br)



<b>PROPÓSITOS E PARÂMETROS</b>	<b>5</b>
--------------------------------	----------

## **1. PANORAMA LEGISLATIVO** 5

<b>Quadro 1: Limites gerais à vigilância sobre as comunicações no Brasil</b>	<b>5</b>
--	----------

<b>Quadro 2: Marco Institucional</b>	<b>6</b>
--------------------------------------	----------

<b>Quadro 3: Vigilância do Estado brasileiro sobre as comunicações</b>	<b>7</b>
--	----------

<b>Quadro 4: Cooperação Jurídica Internacional em matéria penal</b>	<b>8</b>
---	----------

## **2. ANÁLISE: TRUNFOS E PROBLEMAS** 9

<b>Fragilidades de nível constitucional na proteção contra vigilância indevida</b>	<b>9</b>
--	----------

Controvérsias: que sigilo protegemos?	9
---------------------------------------	---

Gradações de privacidade: informações cadastrais <i>metadados</i> conteúdo?	10
---	----

<b>ANATEL: vigilância sem querer querendo</b>	<b>11</b>
---	-----------

Obrigações de prestadores de serviços de telecomunicações	11
---	----

Acesso direto a dados	13
-----------------------	----

<b>Receita Federal: vigilância das comunicações nas entrelinhas</b>	<b>13</b>
---	-----------

<b>Vigilância sem e com contrapesos: Telefonia vs. Internet</b>	<b>14</b>
---	-----------

Lei das Organizações Criminosas (Lei nº 12.850/13)	14
--	----

Obrigação de guarda de registros telefônicos	14
--	----

Prerrogativas de acesso a dados cadastrais	14
--	----

Prerrogativa de acesso também a registros telefônicos?	15
--	----

Marco Civil da Internet (Lei 12.965/14)	16
---	----

Obrigações de guarda de dados	16
-------------------------------	----

Prerrogativas de acesso a dados cadastrais	17
--	----

Acesso a registros de conexão à Internet e de acesso a aplicações	18
---	----

Acesso a comunicações privadas armazenadas	18
--	----

Casos relevantes	19
------------------	----

Ampliando vigilância na falta de regulação para a telefonia	19
---	----

Marco Civil limitando a vigilância na Internet	19
--	----

<b>Interceptações: vigilância limitada na teoria, mas abrangente na prática</b>	<b>20</b>
A teoria: Lei das Interceptações Telefônicas e Resoluções do CNJ e do CNMP	20
A prática: cultura de interceptações	21
<i>Caso Escher e outros vs. Brasil</i> –	
Corte Interamericana de Direitos Humanos	21
Software espião da polícia em celulares grampeados?	22
Sistema Nacional de Controle de Interceptações	22
<b>Vigilância sem transparência para fins de inteligência e segurança nacional</b>	<b>24</b>
A abrangência do Sisbin	24
<i>Cooperação com o Hacking Team?</i>	
Contribuição da Artigo 19 e da Oficina Antivigilância	25
<b>Vigilância sobre comunicações públicas</b>	<b>26</b>
Risco à liberdade de expressão: #HumanizaRedes	26
Rondas Virtuais: a polícia no Facebook –	
Contribuição da Artigo 19 e da Oficina Antivigilância	27
“Mosaico” da ABIN: menos transparência, mais obscuridade	28
<b>3. RECOMENDAÇÕES</b>	<b>29</b>

# PROPÓSITOS E PARÂMETROS

O objetivo deste relatório é apresentar leis e práticas brasileiras relevantes em matéria de vigilância das comunicações pelo Estado e a proteção a direitos fundamentais. São identificados seus trunfos e principais problemas e feitas recomendações, tendo como referência os Princípios Internacionais sobre a Aplicação de Direitos Humanos na Vigilância das Comunicações<sup>1</sup>. Para os fins desta pesquisa, entende-se por vigilância das comunicações interceptações, monitoramento, análise, uso, guarda e obtenção de informações que incluam ou reflitam comunicações passadas, presentes ou futuras de alguma pessoa ou que surjam delas.

<sup>1</sup> <https://pt.necessaryandproportionate.org/text>



# 1. PANORAMA LEGISLATIVO



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 práticas de vigilância envolvendo o Estado brasileiro podem ter pela cooperação judiciária internacional em matéria penal.

### Quadro 1: Limites gerais à vigilância sobre as comunicações no Brasil

<b>DIREITOS</b>	Constituição Federal protege a liberdade de expressão, a intimidade e o sigilo das comunicações (art. 5º incisos IX, X e XI).
	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.
	Não há testes consagrados, de aplicação uniformizada na jurisprudência e na doutrina, para avaliação da constitucionalidade de restrições a esses direitos.
	O art. 5º, § 2º da Constituição Federal dispõe que direitos e garantias 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.
<b>REMÉDIOS</b>	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.
<b>GARANTIAS</b>	Constituição Federal garante o devido processo legal, o contraditório e a ampla defesa, e a presunção de inocência (art. 5º, LIV, LV e LVII). Código de Processo Penal ordena que o juiz observe os princípios da adequação, da necessidade e da proporcionalidade ao ordenar produção de provas (art. 156). O mesmo vale para a apreciação de pedidos de medidas cautelares de produção de provas (art. 282). Intimação do atingido deve sempre ocorrer "ressalvados casos de urgência e de perigo de ineficácia" (art. 282, § 3º).
	Pela Constituição Federal (art. 5º, LVI) e pelo Código de Processo Penal (art. 157) são inadmissíveis provas obtidas por meios ilícitos, contrariando a Constituição ou a lei. Não podem ser aproveitadas.
<b>SANÇÕES</b>	Art. 10 da Lei nº 9.296/96 criminaliza interceptações ilegais e quebra de sigilo de justiça. Pena: reclusão de 2 a 4 anos e multa.
	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.

## Quadro 2: Marco Institucional

<b>ANATEL</b>	Criada pela Lei nº 9.472/97, é órgão regulador responsável por organizar a exploração do setor de telecomunicações e fiscalizar a prestação de serviços a ele relacionados (art. 8º). Pode expedir resoluções (art.19).
	Para o exercício de suas funções e por meio das resoluções, cria obrigações de guarda de dados, de identificação de usuários e de disposição de recursos para vigilância, e institui prerrogativas próprias de acesso a dados guardados.
<b>RECEITA FEDERAL</b>	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.
<b>AUTORIDADES POLICIAIS</b>	São órgãos de segurança. Pela Constituição Federal (art. 144), Polícias Cíveis 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).
	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).
<b>MINISTÉRIO PÚBLICO</b>	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).
	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).
<b>AUTORIDADES JUDICIAIS</b>	Juizes 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.
<b>CPIs</b>	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.
<b>ABIN e Sisbin</b>	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.
	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.

### 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)
<b>OBRIGAÇÕES DE GUARDA DE DADOS</b>	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.	Não há obrigação de guarda expressamente para fins de inteligência.
	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.		
<b>ACESSO A DADOS GUARDADOS (informações cadastrais e metadados)</b>	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.  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. Pelo MS 23452/RJ do STF, acesso a registros telefônicos também pode ocorrer no âmbito de CPIs.	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.
		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).	

### Quadro 3: Vigilância do Estado brasileiro sobre as comunicações

<b>ACESSO A COMUNICAÇÕES DOCUMENTADAS</b>	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). Segundo RE 418.416-8/SC, julgado pelo STF, mandado de busca e apreensão legitimiza 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.
<b>INTERCEPTAÇÕES</b>	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).

### Quadro 4: Cooperação Jurídica Internacional em matéria penal

<b>ACORDOS DE COOPERAÇÃO INTERNACIONAL EM MATÉRIA PENAL</b>	
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.	
<b>Exigem dupla incriminação</b>	Acordos bilaterais com China, Coreia do Sul, Cuba, França e Portugal
<b>Exigem dupla incriminação em exceções</b>	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
<b>Não exigem dupla incriminação</b>	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-incriminacao-na-cooperacao-juridica-internacional](http://www.ibccrim.org.br/boletim_artigo/4678-Dupla-incriminacao-na-cooperacao-juridica-internacional) Acesso: 31.07.15.



## 2. ANÁLISE: VIRTUDES E PROBLEMAS



## 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 da 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 a 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 Federal brasileira proteger o sigilo das comunicações e a privacidade, questões interpretativas ameaçam a efetividade da proteção que esses direitos garantem contra a vigilância indevida de autoridades do Estado sobre comunicações.

### CONTROVÉRSIAS: QUE SIGILO PROTEGEMOS?

Em primeiro lugar, está a controvérsia sobre o âmbito de proteção do pouco claro 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”), central para a proteção do sigilo das comunicações, agravada diante da ausência de teste consagrado na jurisprudência e na doutrina para avaliação da constitucionalidade de restrições a direitos fundamentais, o que torna a apreciação das restrições bastante casuística.

De modo geral, as discussões interpretativas sobre o inciso XII se dão em dois níveis: (i) disputa-se se o objeto de proteção desse direito fundamental são as informações comunicadas transmitidas pelos meios em questão (correspondências, mensagens telegráficas, dados e telefonemas em si) ou a comunicação, ou seja, o fluxo dessas informações; (ii) diverge-se acerca de quais os grupos, dentre os quatro listados no inciso, estão submetidos à exceção constitucional que permite a quebra do sigilo (“salvo, no último caso...”). O entendimento doutrinário predominante<sup>2</sup>, já evidenciado em decisão Supremo Tribunal Federal<sup>3</sup>, é no sentido de 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 seu fluxo enquanto ocorrem e que 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.

<sup>2</sup> 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.

<sup>3</sup> 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. 5º ao fluxo de dados.

Grande parte dessas controvérsias orienta-se em identificar um núcleo de proteção absoluta do art. 5º, inciso XII, cuja restrição seria sempre inconstitucional: pelo entendimento apresentado acima, comunicações por correspondências, enquanto em fluxo, por exemplo, seriam absolutamente invioláveis. Tal posicionamento, mesmo que encontrado na doutrina, não reflete a jurisprudência dos tribunais, que já admitiu “quebras” do sigilo do fluxo das comunicações de todos os tipos, desde que “proporcionais”, quando se fundamentarem em direito fundamental concorrente ou em interesse público.<sup>4</sup> Ao mesmo tempo, o entendimento restrito que adotam, como o de que apenas o fluxo de comunicações seria protegido pelo art. 5º, inciso XII, se mostra insuficiente para proteger adequadamente o conteúdo de comunicações armazenadas, registradas ou gravadas ou mesmo de informações geradas a respeito das circunstâncias em que ocorreram as comunicações (metadados). Essa interpretação conflita com aquela adotada pela Corte Interamericana de Direitos Humanos no caso *Escher e outros vs. Brasil*, conforme detalhado na seção 2.5 deste relatório.

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

Mesmo que apenas o fluxo das comunicações seja tido como objeto de proteção do inciso XII do art. 5º na jurisprudência e na doutrina, o direito à privacidade, previsto genericamente no inciso X do mesmo artigo, permite a proteção das comunicações de maneira mais ampla<sup>5</sup>, isto é, não só do seu conteúdo, mas também das informações sobre as circunstâncias em que ocorreram e entre quem se deram (o que pode ser revelado por informações cadastrais<sup>6</sup> e metadados<sup>7</sup>). Como se verá adiante, 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. Contudo, essas distinções podem não ser mais adequadas para mensurar o grau de intromissão que a vigilância das comunicações acarreta para pessoas e organizações. É por essa razão que acadêmicos e especialistas em privacidade de mais de 70 países defendem, por meio dos Princípios Internacionais sobre a Aplicação de Direitos Humanos na Vigilância das Comunicações, que não só o conteúdo das comunicações receba proteção mas também que sejam protegidos, em igual medida, os metadados sobre essas comunicações uma vez que podem revelar informações até mesmo mais sensíveis do que o próprio conteúdo da comunicação em si.

Apesar disso, a legislação brasileira ainda não garante o mesmo nível de proteção para informações não relacionadas ao conteúdo das comunicações. Para informações cadastrais, por exemplo, o entendimento que parece predominar 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

<sup>4</sup> No habeas corpus 70814/SP (Min. Rel. Celso de Mello, julg. em 01.03.2004), por exemplo, o Supremo Tribunal Federal admitiu, por exemplo, 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 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.

<sup>6</sup> Para fins deste relatório, consideram-se informações cadastrais todas aquelas que constarem do cadastro do cidadão junto à empresa de telefonia, administrador de sistema autônomo ou provedor de aplicações.

<sup>7</sup> Para fins deste relatório, consideram-se metadados todos aqueles dados e registros gerados a partir da comunicação e que não sejam 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 do dispositivo (como IMEI), etc.

informações por mera requisição de autoridades, retirando a necessidade de ordem judicial.<sup>8</sup> Talvez isso possa ser parcialmente explicado como uma repercussão inapropriada do argumento da “vedação constitucional ao anonimato”, prevista no inciso IV do art. 5º, que, embora devesse estar relacionado apenas a casos de manifestação do pensamento, tem justificado a necessidade de acesso a esses dados para identificação de responsáveis em quaisquer casos.

Para quebra de sigilo de metadados, cujo tratamento legislativo varia conforme se refiram ao uso de telefonia ou de Internet, em geral basta ordem judicial fundamentada. Já para a realização de interceptações, ou seja, para que se tenha acesso ao conteúdo das comunicações em si, por outro lado, 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, diante disso, fragilizados.

## **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.

## **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.

<sup>8</sup> Alterações legislativas recentes “contornam” necessidade de ordem judicial para obtenção de dados cadastrais, como se verá adiante neste relatório (item 2.4: 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: 17.06.15.



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, “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.

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 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.

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.<sup>9</sup>

## **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<sup>10</sup> 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

<sup>9</sup> 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 31.07.15.

<sup>10</sup> FOLHA DE SÃO PAULO, “Anatel terá acesso total a dado sigiloso de telefones”, publicada em 19.01.11. Disponível em: <http://www1.folha.uol.com.br/fsp/mercado/me1901201103.htm> Acesso em: 17.06.15.

que o acesso a registros de chamadas somente ocorreria com autorização de usuário que fizesse reclamação à agência<sup>11</sup> e que os software a serem instalados permitiriam apenas fornecimento de “informações em estado bruto” das prestadoras, não conectadas a dados cadastrais.<sup>12</sup> 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.

## 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 recente 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.<sup>13</sup> Considerando que a Receita Federal tem acesso a informações sobre comunicações de brasileiros, essa cooperação pode significar ampliação da vigilância.

<sup>11</sup> FOLHA DE SÃO PAULO, “Agência diz que não há quebra de sigilo”, publicada em 19.01.11. Disponível em <http://www1.folha.uol.com.br/fsp/mercado/me1901201104.htm> Acesso em: 17.06.15

<sup>12</sup> GAZETA DO POVO, “Quebra de sigilo continua a depender de mandado judicial, diz Anatel”, publicada em 21.01.11. Disponível em: <http://www.gazetadopovo.com.br/economia/quebra-de-sigilo-continua-a-depender-de-mandado-judicial-diz-anatel-da8drvp4kj7uyodcxir2ijw3y> Acesso em: 17.06.15.

<sup>13</sup> Sobre isso, ver VARON FERRAZ, Joana., Boletim n. 11 da Oficina Antivigilância, disponível em <https://antivigilancia.org/pt/2015/07/novas-revelacoes-do-wikileaks-sobre-vigilancia-no-brasil-dilma-disse-que-nao-tem/>. Refere-se a acordo disponível em [http://www.itamaraty.gov.br/index.php?option=com\\_content&view=article&id=10389:atos-assinados-por-ocasio-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](http://www.itamaraty.gov.br/index.php?option=com_content&view=article&id=10389:atos-assinados-por-ocasio-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: 31.07.15

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

Leis federais recentes normatizaram capacidades de vigilância do Estado no exercício de 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)**

#### **Obrigaç o de guarda de registros telef nicos**

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 recentemente pela Lei nº 12.683/2012.

Cabe destacar aqui que 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, e a Lei Complementar nº 75/93, em seu art. 8º, inciso IV, permitir ao Ministério Público da União a requisição de “informações e documentos a entidades privadas” no exercício de suas atribuições, o que se aplica subsidiariamente aos organismos estaduais (art. 80 da Lei nº 8.625/93), o acesso a tais informações era rejeitado pelas empresas com base no argumento

de que estariam protegidas pela proteção constitucional da privacidade do art. 5º, inciso X, da Constituição Federal, sendo necessária ordem judicial para quebra do sigilo.<sup>14</sup> Nesse contexto, os recentes dispositivos atendem a pressões das autoridades investigativas para ter o “livre acesso” – por mera requisição – expressamente legislado, o qual contribuiria para a eficácia, em termos de rapidez, de investigações e processos. Cabe ressaltar ainda 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.<sup>15</sup> 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 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. 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.<sup>16</sup> A ação ainda está pendente de julgamento.

<sup>14</sup> 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: 17.06.15.

<sup>15</sup> Ver 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](http://www.ibccrim.org.br/boletim_artigo/4671-A-investigao-criminal-na-nova-lei-de-lavagem-de-dinheiro) Acesso em: 17.06.15.

<sup>16</sup> 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”, de 29.10.14, 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: 31.07.15.

## MARCO CIVIL DA INTERNET (LEI 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 Liveo 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.<sup>17</sup> Objeto da guarda, os registros de conexão, são, segundo o art. 5º, inciso VI, “o conjunto de informações referentes à data e hora de início e término de uma conexão à Internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados”. O art. 14, em atenção aos riscos à privacidade de usuários da rede, proíbe que provedores de conexão guardem registros de acesso a aplicações.

O art. 15 do Marco Civil da Internet determina, por sua vez, que “o provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento”. Aplicações, segundo inciso VII do art. 5º, são o “conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet”. 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 três 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 regulamento a que se referem os arts. 13 e 15, que, possivelmente, trará mais especificações quanto a destinatários da obrigação do art. 15, ao prazo máximo de guarda e a medidas de segurança, ainda não foi editado; já passou, contudo, por fase inicial de consulta pública, na forma de coleta de contribuições e debates, e se encontra em fase de sistematização. Dele se espera aumento da proteção contra vigilância indevida.

<sup>17</sup> 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 instituiu a obrigação da guarda de registros de conexão.

## **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 têm solicitado que o decreto regulamentador do Marco Civil da Internet esclareça os limites desse acesso, delimitando expressamente as autoridades competentes, seja exigindo relação entre autoridade requerente e fundamentação do pedido e/ou restringindo o acesso sem autorização judicial, limitando-o aos termos das Leis das Organizações Criminosas e de Lavagem de Dinheiro, de modo a evitar abusos na solicitação dessas informações.<sup>18</sup> Também espera-se que o decreto se manifeste 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.<sup>19</sup>

## **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 sigilo de justiça, inclusive quanto aos pedidos de guarda de registro”.

## **Acesso a comunicações privadas armazenadas**

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. Tais dispositivos, ao lado do art. 11, que preceitua a obrigação de respeito à legislação brasileira a provedores que coletam, guardam e tratam dados no Brasil, atenderam a dificuldades práticas na quebra de sigilo telemático (emails, principalmente), 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 tinham argumentos mais fortes para se opor e não realizar a quebra de sigilo, recusando-se a obedecer ordens judiciais.<sup>20</sup> Em face disso, o § 2º do art. 11 expressamente previu que “o disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo

<sup>18</sup> Ver BRITO CRUZ, Francisco, et. al., “O que está em jogo na regulamentação do Marco Civil?”, p. 32. Disponível em <http://www.internetlab.org.br/wp-content/uploads/2015/08/Report-MCI-v2-ptbr.pdf> Último acesso em 13 setembro 2015.

<sup>19</sup> 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](https://antivigilancia.org/boletim_antivigilancia/consultas/visualizacao). Acesso em: 17.06.15.

<sup>20</sup> Essa argumentação foi utilizada pelo Google em inúmeros casos. Antes do Marco Civil da Internet, o Superior Tribunal de Justiça, no Inquérito n. 784-DF (Min. Laurita Vaz, julg. 17.03.13) se manifestou sobre o assunto, ordenando a exibição dos dados.

econômico possua estabelecimento no Brasil.” Assim, se, de um lado, o Marco Civil da Internet consagrou a proteção por ordem judicial para este tipo de produção de prova, de outro, estendeu as capacidades de vigilância do Estado brasileiro. Tal previsão tem encontrado obstáculos para sua efetividade na prática. A inclusão desses dispositivos não solucionou, contudo, os problemas de jurisdição que podem surgir uma vez que os provedores ainda podem questionar a aplicação da legislação brasileira a dados armazenados no exterior, o que tem dado margem a decisões judiciais controversas e/ou desproporcionais.<sup>21</sup>

## CASOS RELEVANTES

### Ampliando vigilância na falta de regulação para a telefonia

A vigilância da telefonia para fins de 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 fazê-lo, teve sua prisão decretada. Sua localização foi tentada repetidas vezes, sem sucesso. Em face disso, e em nome da “proteção integral a crianças e adolescentes”, a desembargadora admitiu que uma “interceptação telefônica”, como a chamou, fosse efetuada com o fim de levantar dados sobre a localização do devedor a partir de seu número de celular.<sup>22</sup>

### Marco Civil limitando a vigilância na Internet

O Marco Civil da Internet, por outro lado, já soma frutos em termos de limitação contra vigilância indevida. A Justiça Federal de São Paulo anulou, em decisão de abril de 2015<sup>23</sup>, 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

<sup>21</sup> Em fevereiro de 2015 o juiz Luiz Moura Correia da Central de Inquéritos da Comarca de Teresina ordenou a suspensão do aplicativo WhatsApp em todo o Brasil, porque a companhia não estaria colaborando com investigações criminais e respeitando ordens de quebras de sigilo. Ver notícia em O ESTADO DE SÃO PAULO, “Juiz exige a suspensão do Whatsapp no Brasil”, publicada em 25.02.15, disponível em <http://blogs.estadao.com.br/link/juiz-exige-a-suspensao-do-whatsapp-no-brasil/> (Acesso em 31/07/2015). A decisão foi anulada no Tribunal de Justiça do Piauí pouco depois. Ver também, mais recentemente, caso envolvendo a Yahoo Inc, tratado no Blog do InternetLab no jornal o Estado de São Paulo em 23.07.15, disponível em <http://blogs.estadao.com.br/deu-nos-autos/acesso-daqui-guardo-la-onde-estao-nossos-dados-na-internet/> Acesso em 31.07.15

<sup>22</sup> 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: 17.06.15.

<sup>23</sup> 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](http://www.omci.org.br/m/jurisprudencias/arquivos/2015/jfsp_00019729120154036100_24042015_KG45KXb.pdf) Acesso em: 17.06.15.

Civil da Internet “prevê a possibilidade de requisição de dados cadastrais pelas autoridades administrativas e a Lei n. 12.830/2013 expressamente autoriza que os Delegados de Polícia, no curso do inquérito policial, requisitem dados e informações de interesse às investigações”, em referência ao art. 2º, § 2º de tal lei. Em sua decisão, o juiz federal reconhece que a requisição feita pela autoridade policial abrange não apenas dados cadastrais de usuários, mas também registros de acesso a aplicação e afirma: “a lei [o Marco Civil] permite às autoridades administrativas, com competência para tanto, requisitar informações aos provedores de internet referentes aos seus usuários, desde que tais informações se limitem a dados cadastrais, como qualificação pessoal, filiação e endereço. Entendo, pois, que informações relacionadas aos registros de conexão e de acesso a aplicações de internet, bem como de dados pessoais e do conteúdo de comunicações privadas, dependem de autorização judicial, como expressamente previsto no referido § 1º, do art. 10, da Lei nº 12.965/14.” No que se refere aos dados cadastrais, o juiz acolhe esclarecimento do Twitter no sentido de que não possuiria informações como nome completo, endereço e filiação do usuário, e, quanto aos registros de acesso a aplicação, rejeita a obrigação de disponibilização dos dados, dada a ausência de ordem judicial que a ampare.

## **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.<sup>24</sup> Entretanto, em razão de vício formal, a Ação Direta de Inconstitucionalidade proposta não foi julgada no mérito. 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 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

<sup>24</sup> SUPREMO TRIBUNAL FEDERAL. Ação Direta de Inconstitucionalidade n. 1488-9/DF, Min. Néri da Silveira, julg. em 07.11.1999.



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<sup>25</sup>, prevalece o entendimento de que a medida pode ser estendida *enquanto* indispensável. O art. 7º dá à autoridade policial o poder de requisitar “serviços e técnicos especializados às concessionárias de serviço público” para os procedimentos de interceptação. O art. 8º ordena o sigilo no tratamento das gravações e o art. 9º, a sua inutilização, quando não interessarem a fins de prova. Interceptações ilegais são criminalizadas no art. 10. Por tudo isso, pode-se dizer que, em geral, a Lei de Interceptações 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.<sup>26</sup> 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 sigredo de justiça foram vazados e, a seguir, intencionalmente divulgados em coletiva de imprensa convocada pelo Secretaria de Segurança Pública do Paraná dias após as

<sup>25</sup>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).

<sup>26</sup> 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](http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf) Acesso em: 17.06.15.

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.

A CIDH também reconheceu expressamente que o direito à privacidade abarca não só a proteção do conteúdo das comunicações mas também dos metadados: “[O direito à privacidade] aplica-se às conversas telefônicas independentemente do conteúdo destas, inclusive, pode compreender tanto as operações técnicas dirigidas a registrar esse conteúdo, mediante sua gravação e escuta, como qualquer outro elemento do processo comunicativo, como, por exemplo, o destino das chamadas que saem ou a origem daquelas que ingressam; a identidade dos interlocutores; a frequência, hora e duração das chamadas; ou aspectos que podem ser constatados sem necessidade de registrar o conteúdo da chamada através da gravação das conversas. Finalmente, a proteção à vida privada se concretiza com o direito a que sujeitos distintos dos interlocutores não conheçam ilicitamente o conteúdo das conversas telefônicas ou de outros aspectos, como os já elencados, próprios do processo de comunicação.”<sup>27</sup>

### **Software espião da polícia em celulares grampeados?**

Em abril de 2015, o jornal Folha de São Paulo revelou que a Polícia Federal está tentando ampliar o acesso a informações armazenadas em telefones celulares sob interceptação judicialmente autorizada.<sup>28</sup> 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 que a Polícia Federal “quer que empresas de telefonia adquiram os programas espiões”, o que tem sido recebido com resistência por elas em razão dos custos dos programas e da utilização do pacote de dados dos investigados para transferência das informações copiadas. Além disso, a notícia também afirma que, durante a Operação Lava Jato, que deflagrou escândalo de corrupção na Petrobras, a Polícia Federal só conseguiu devassar mensagens de investigado, o doleiro Alberto Youssef, “porque conseguiu convencer a BlackBerry a franquear acesso às conversas feitas por BBM, serviço de mensagens instantâneas dos aparelhos da marca”.

A notícia evidencia, 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 do 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 a notícia diz respeito, desperta preocupações que vão além do sigilo das comunicações e afetam a integridade das comunicações e sistemas.<sup>29</sup> (Sobre isso,

<sup>27</sup> 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](http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf) Acesso em: 17.06.15.

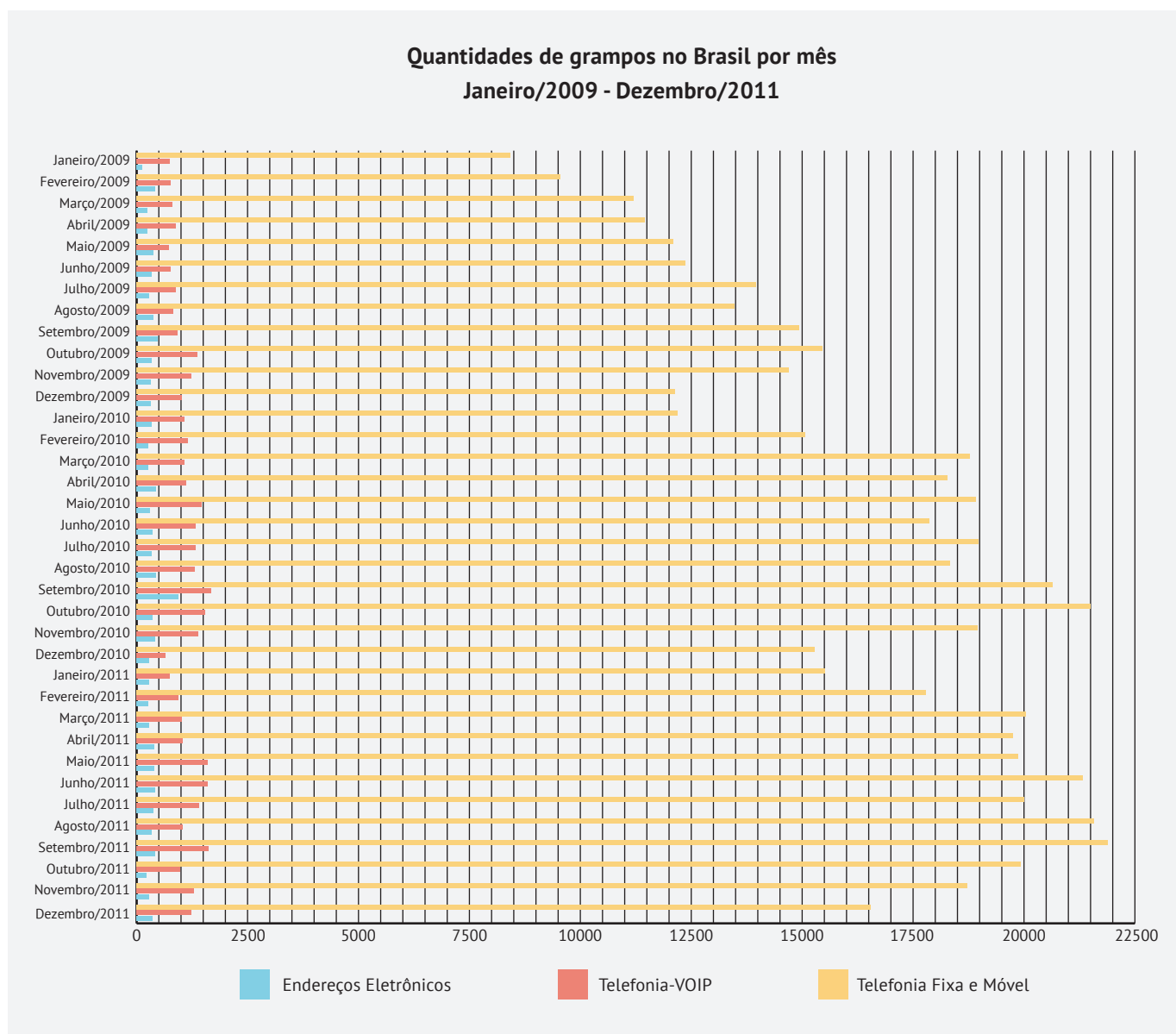
<sup>28</sup> FOLHA DE SÃO PAULO, “PF quer instalar vírus em telefone grampeado para copiar informações”, publicada em 27.04.15. Disponível em: <http://www1.folha.uol.com.br/poder/2015/04/1621459-pf-quer-instalar-virus-em-telefone-grampeado-para-copiar-informacoes.shtml> Acesso em 17.06.15.

<sup>29</sup> Sobre o tema, ver MENDES, Laura Schertel, “Uso de softwares espiões pela polícia: prática legal?”, in: Jota, publicada em 04.06.2015, 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 o item Cooperação com o Hacking Team?, adiante). De outro lado, a notícia também mostra como a deficiência legislativa dá lugar a “acordos” extralegais na obtenção de dados protegidos pelos direitos ao sigilo das comunicações e à privacidade.

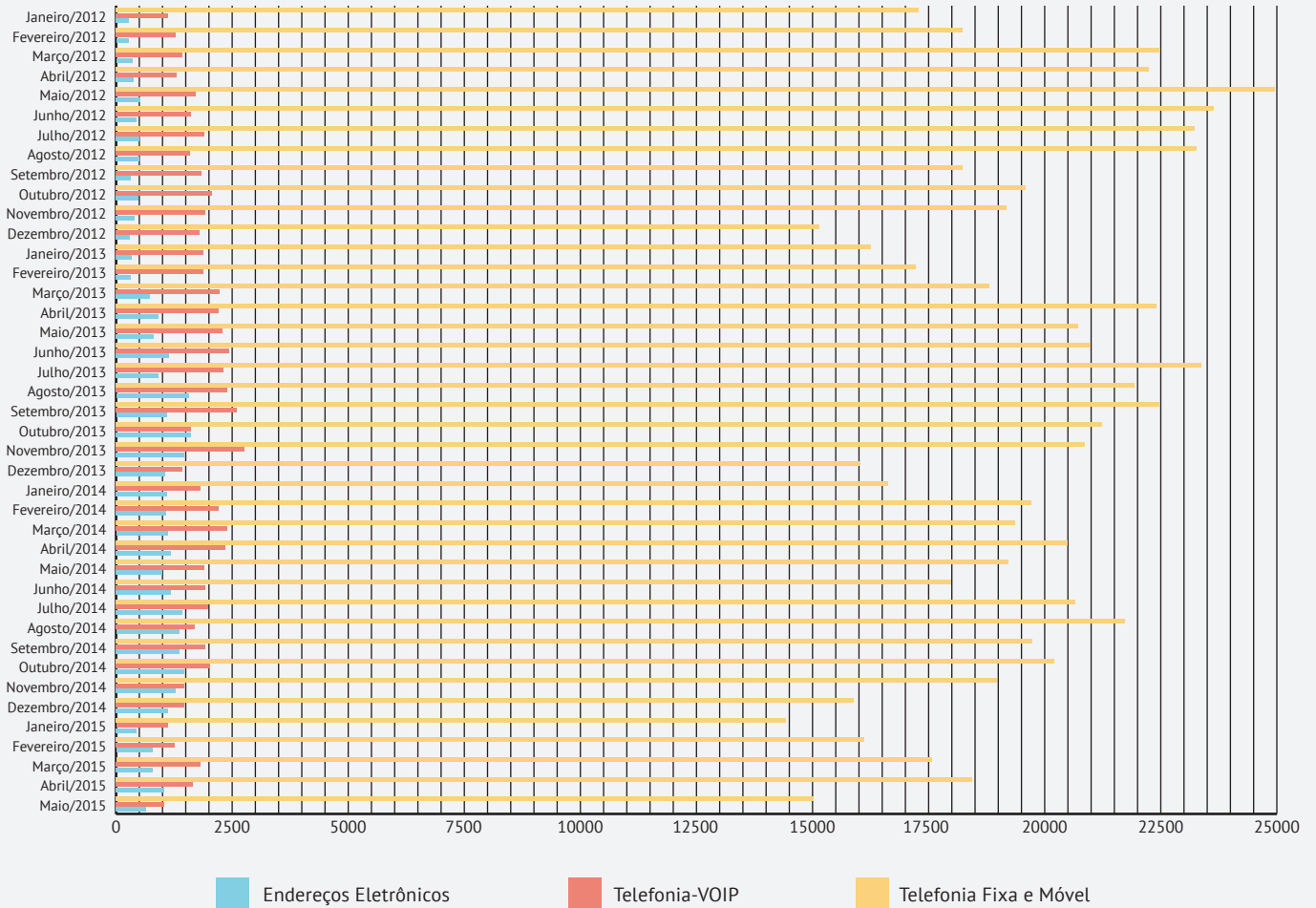
### Sistema Nacional de Controle de Interceptações

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”, que recolhe informações sobre ofícios expedidos a prestadoras de serviço, procedimentos instaurados e quantidade de telefones, telefones-VOIP e emails monitorados. Tais dados não estão disponíveis publicamente e foram obtidos pelo InternetLab por meio da Lei de Acesso à Informação.<sup>30</sup>

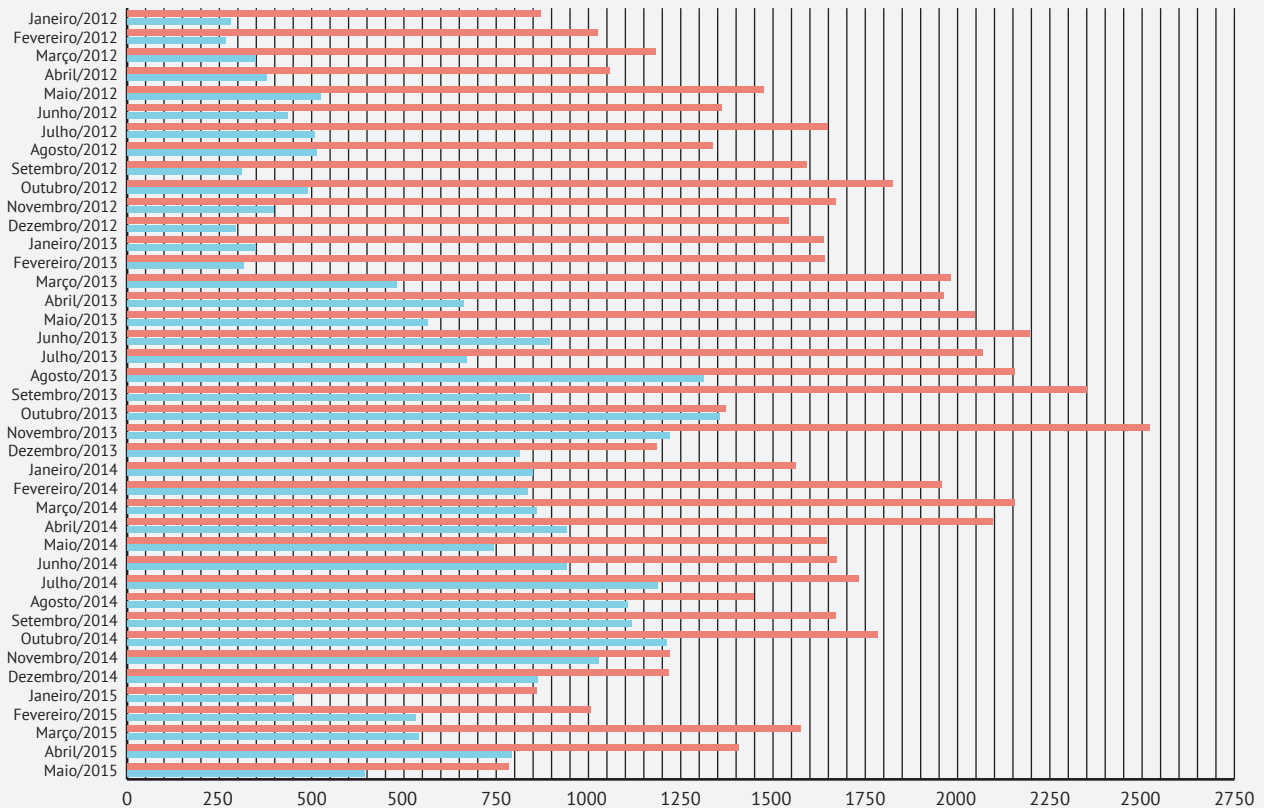
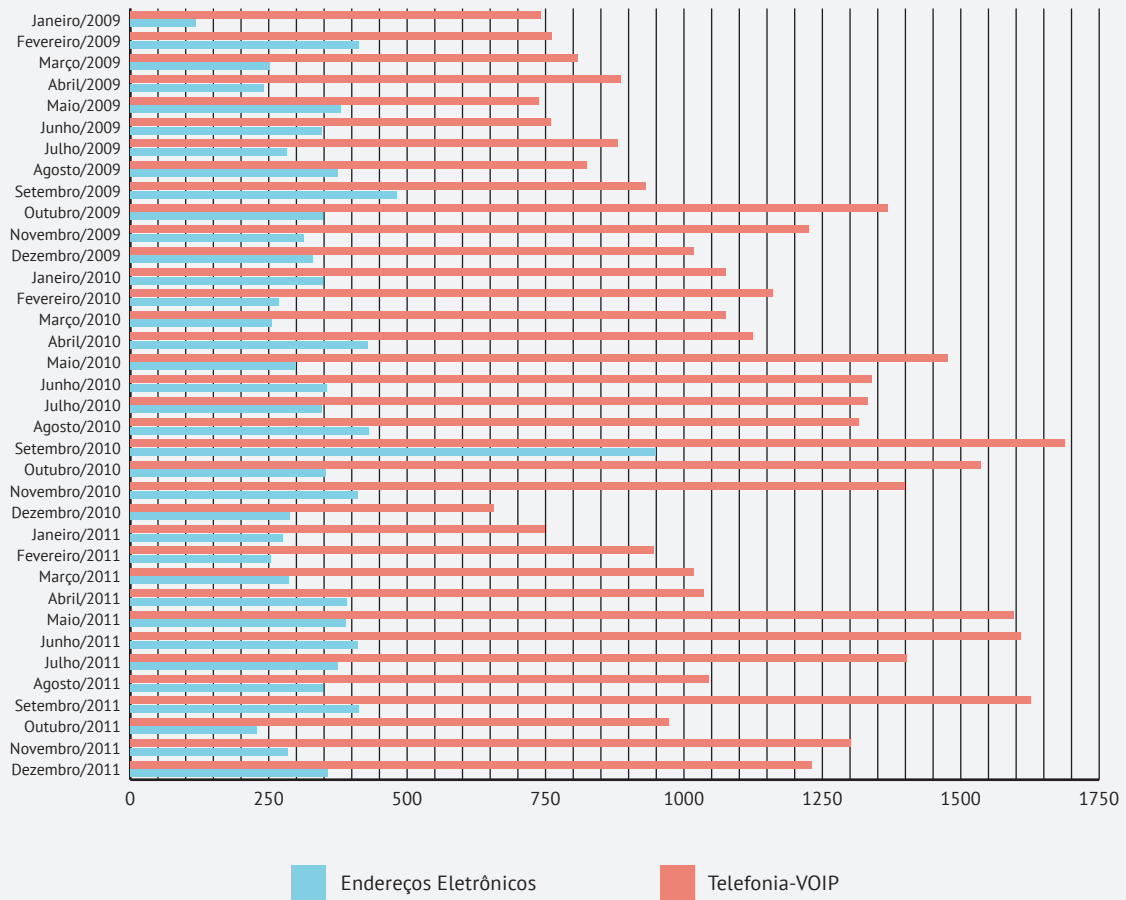


<sup>30</sup> Registro na Ouvidoria/CNJ: 147763. Pedido realizado pelo InternetLab ao Conselho Nacional de Justiça e respectiva resposta, incluindo dados completos do sistema, disponível em <http://www.internetlab.org.br/wp-content/uploads/2015/07/LAI-Interceptações-para-o-site.pdf>. (Acesso em: 03.08.15)

### Quantidades de grampos no Brasil por mês Janeiro/2012 - Maio/2014



### Quantidades de grampos no Brasil por mês



Os gráficos mostram que a média mensal de linhas de telefone monitoradas no Brasil ultrapassa 18 mil. Também se nota que a quantidade de endereços eletrônicos e telefones voice over IP tem crescido nos últimos meses. Para dizer o que esses números e os demais recolhidos no Sistema Nacional de Controle de Interceptações 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 Sistema Nacional de Controle de Interceptações.

A comparação com outros países tampouco ajuda nessa avaliação, dada a ausência de critérios equivalentes na realização 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 2013, foi de 3.576<sup>31</sup>. Não há informações quanto à quantidade de interceptações deferidas no Brasil; o que se sabe é que 13.309 procedimentos criminais novos de interceptação foram instaurados em 2013.<sup>32</sup> 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 2013 foi de 19.398.<sup>33</sup> Sobre o Brasil, o que se sabe é que 50.265 ofícios de interceptação foram expedidos a empresas de telecomunicações nesse período.<sup>34</sup>

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.

## 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

<sup>31</sup> Ver estatísticas disponíveis em <http://www.uscourts.gov/statistics-reports/wiretap-report-2013> Acesso em 03.08.15.

<sup>32</sup> Ver dados do Sistema Nacional de Interceptações disponíveis em <http://www.internetlab.org.br/wp-content/uploads/2015/07/LAI-Interceptações-para-o-site.pdf>. Esse número se refere à quantidade de procedimentos criminais instaurados em 2013, 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 2013 referentes ao item „Total 3”, relativas a interceptações telefônicas, somadas às do item „Total 9”, relativas a interceptações telemáticas.

<sup>33</sup> Ver estatísticas disponíveis em: [https://www.bundesjustizamt.de/DE/SharedDocs/Publikationen/Justizstatistik/Uebersicht\\_TKUE\\_2013.pdf?\\_\\_blob=publicationFile&v=3](https://www.bundesjustizamt.de/DE/SharedDocs/Publikationen/Justizstatistik/Uebersicht_TKUE_2013.pdf?__blob=publicationFile&v=3) Acesso em 03.08.15.

<sup>34</sup> Ver dados do Sistema Nacional de Interceptações disponíveis em <http://www.internetlab.org.br/wp-content/uploads/2015/07/LAI-Interceptações-para-o-site.pdf>. Esse número se refere à quantidade de ofícios expedidos em 2013, 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 2013 referentes ao item „Total 1”, relativas a interceptações telefônicas, somadas às do item „Total 7”, relativas a interceptações telemáticas.

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, 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 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). 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. Apesar de não poder realizar diretamente interceptações, por exemplo, por não ter sido contemplado o fim de inteligência na Constituição nem na Lei das Interceptações<sup>35</sup>, o acesso a dados por meio de cooperação não 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 Guardiã da Polícia Federal.<sup>36</sup> 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). 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.

<sup>35</sup> Esse entendimento é afirmado na jurisprudência. Ver SUPERIOR TRIBUNAL DE JUSTIÇA, HC 149250-SP, Min. Rel. Adilson Vieira Macabul julg. 16.05.12, que considerou interceptações realizadas com participações de agentes da ABIN no âmbito da Operação Satiagraha ilegais. É também o manifestado publicamente pela ABIN. Em resposta à pergunta "A ABIN faz escuta telefônica?" em seu site, o que se lê é "Não. A Lei 9.296, de 24 de julho de 1996, que regulamenta o dispositivo constitucional, art. 5º, inciso XII, estabelece os órgãos competentes para executar, com autorização judicial, a interceptação telefônica. A ABIN não se enquadra nessa determinação legal." Disponível em: [http://www.abin.gov.br/modules/mastop\\_publish/?tac=Perguntas\\_Frequentes](http://www.abin.gov.br/modules/mastop_publish/?tac=Perguntas_Frequentes) (Acesso em: 31.07.15). 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", publicado em 07.11.08, disponível em <http://www1.folha.uol.com.br/fsp/corrida/cr0709200802.htm> (Acesso em: 31.07.15).

<sup>36</sup> FOLHA DE SÃO PAULO, "Acesso ao Guardiã pela Abin gera polêmica", publicada em 12.11.08. Disponível em: <http://www1.folha.uol.com.br/fsp/brasil/fc1211200805.htm> Acesso em: 17.06.15.

## COOPERAÇÃO COM O HACKING TEAM? – CONTRIBUIÇÃO DA ARTIGO 19 E DA OFICINA ANTIVIGILÂNCIA

No dia 5 de Julho de 2015, a empresa italiana Hacking Team - conhecida por desenvolver e vender softwares espíões e ferramentas de vigilância para governos, e ajudar instituições policiais e militares a espionar computadores, tablets e celulares de cidadãos e cidadãs em todo o mundo - foi hackeada. Como resultado, 400GB de documentos internos, entre eles emails privados, faturas, lista de clientes e códigos fonte dos produtos comercializados, foram divulgados na Internet.

Na documentação vazada, há inúmeras referências a órgãos de inteligência do Brasil, tanto os civis quanto os militares, e a empresas brasileiras que, ao que tudo indica, seriam parceiras locais da Hacking Team. Entre os órgãos que aparecem nos arquivos estão: Agência Brasileira de Inteligência (ABIN)<sup>37</sup>, Centro de Inteligência do Exército (CIE)<sup>38</sup>, Centro de Instrução de Guerra Eletrônica (CIGE)<sup>39</sup>, Polícia Civil do Rio de Janeiro (CINPOL<sup>40</sup> e DRCI<sup>41</sup>), Polícia Militar do Rio de Janeiro<sup>42</sup>, Polícia Civil de São Paulo<sup>43</sup>, Polícia Militar de São Paulo<sup>44</sup>, Polícia Civil do Distrito Federal<sup>46</sup>, Polícia Militar do Distrito Federal<sup>47</sup>, Ministério da Justiça e Procuradoria Geral da República<sup>48</sup>. O arquivo é vasto e exige uma análise cuidadosa, inclusive de veracidade de cada documento, não sendo possível afirmar, até o momento, se as agências citadas chegaram de fato a adquirir as “soluções” da empresa italiana. A única exceção parece ser, no entanto, a Polícia Federal<sup>49</sup>, uma vez que a pesquisa nos arquivos, ainda que superficial, revela trocas de emails entre agentes e funcionários da Hacking Team<sup>50</sup>, relatos sobre treinamentos em Brasília<sup>51</sup>, e diversos documentos, como um certificado de entrega de produto<sup>52</sup>, que confirmam a negociação e aquisição da “solução” RCS (Remote Control System) da Hacking Team para um projeto piloto de 3 meses de duração.

Mesmo que os documentos sejam verdadeiros, ainda não está claro, contudo, que processo administrativo foi seguido para que a aquisição fosse realizada. Nos emails há apenas uma referência à Lei nº 13.097, de 19 de janeiro de 2015, que dispensa a licitação na compra de “equipamentos sensíveis e necessários à investigação policial”. Há também referência a uma ordem judicial<sup>53</sup> que teria sido expedida no primeiro semestre de 2015, dando à Polícia Federal amparo legal para o uso das soluções adquiridas, durante 15 dias (a partir da infecção), em 17 telefones-alvo.

<sup>37</sup> <https://www.wikileaks.org/hackingteam/emails/?q=%22ABIN%22&mfrom=&mto=&title=&notitle=&date=&nofrom=&noto=&count=50&sort=0#searchresult>

<sup>38</sup> <https://www.wikileaks.org/hackingteam/emails/emailid/446716>

<sup>39</sup> <https://www.wikileaks.org/hackingteam/emails/?q=%22CIGE%22&mfrom=&mto=&title=&notitle=&date=&nofrom=&noto=&count=50&sort=0#searchresult>

<sup>40</sup> <https://www.wikileaks.org/hackingteam/emails/?q=%22CINPOL%22&mfrom=&mto=&title=&notitle=&date=&nofrom=&noto=&count=50&sort=0#searchresult>

<sup>41</sup> <https://www.wikileaks.org/hackingteam/emails/?q=%22DRCI%22&mfrom=&mto=&title=&notitle=&date=&nofrom=&noto=&count=50&sort=0#searchresult>

<sup>42</sup> <https://www.wikileaks.org/hackingteam/emails/emailid/7264>

<sup>43</sup> <https://www.wikileaks.org/hackingteam/emails/emailid/7264>

<sup>44</sup> <https://www.wikileaks.org/hackingteam/emails/?q=%22policiamilitar.sp.gov.br%22&mfrom=&mto=&title=&notitle=&date=&nofrom=&noto=&count=50&sort=0#searchresult>

<sup>45</sup> <https://www.wikileaks.org/hackingteam/emails/emailid/237181>

<sup>46</sup> <https://www.wikileaks.org/hackingteam/emails/emailid/446822>

<sup>47</sup> <https://www.wikileaks.org/hackingteam/emails/?q=%22mj.gov.br%22+!%22Progetto+Polizia+Federal%22&mfrom=&mto=&title=&notitle=&date=&nofrom=&noto=&count=50&sort=2#searchresult>

<sup>48</sup> <https://www.wikileaks.org/hackingteam/emails/emailid/446919>

<sup>49</sup> <http://apublica.org/2015/07/hackeando-o-brasil/>

<sup>50</sup> <http://htbrasil.pen.io/>

<sup>51</sup> <https://www.wikileaks.org/hackingteam/emails/emailid/921981>

<sup>52</sup> <https://www.wikileaks.org/hackingteam/emails/emailid/921981> (arquivo em anexo)

<sup>53</sup> <https://www.wikileaks.org/hackingteam/emails/emailid/921908>



O RCS, segundo a própria Hacking Team, é um sistema discreto, baseado em spyware, e desenvolvido para atacar, infectar e monitorar computadores<sup>54</sup> (Windows, MAC OS, Linux) e smartphones (Android, BlackBerry, Windows Phone e iOS com Jailbreak). A ferramenta permite o monitoramento e controle de dados e atividades do dispositivo infectado: é possível ver arquivos armazenados, e quais deles foram abertos recentemente, deletados ou impressos; ligar o microfone e a câmera e capturar imagens ou sons; ter acesso a chats, emails, SMS e localização; ouvir conversas via Skype (VOIP) e ligações de voz; e até capturar tudo o que é digitado no teclado (keystrokes). O RCS possui diversas técnicas de infecção, que podem ser físicas ou remotas: através de pen-drives; redes Wi-Fi; streaming de vídeos; anexos em emails; e simples links para sites falsos.

De forma geral, os documentos vazados trazem mais questionamentos sobre o crescente mercado de vigilância no Brasil, e apontam para a necessidade de considerações legais sobre que tipo de dados podem ser acessados a partir de quebras de sigilo, principalmente levando em conta o avanço das novas tecnologias de vigilância. Os 400GB parecem confirmar, ainda, as informações publicadas em abril de 2015, pelo jornal Folha de São Paulo, sobre a tentativa da Polícia Federal de utilizar, com autorização judicial, “aplicativo especial” para coletar dados de telefones investigados.<sup>55</sup>

## VIGILÂNCIA SOBRE COMUNICAÇÕES PÚBLICAS

A seguir são apresentadas três práticas de monitoramento de comunicações públicas, registradas na Internet. Apesar de não levantar questões sobre o sigilo das comunicações e a privacidade, esse tipo de vigilância de diferentes organismos estatais tem o potencial de impactar negativamente o exercício de liberdades, principalmente, a de expressão, a de reunião e a de associação.

### RISCO À LIBERDADE DE EXPRESSÃO: #HUMANIZAREDES

O Pacto Nacional de Enfrentamento às Violações de Direitos Humanos na Internet - #HumanizaRedes é um programa do Governo Federal brasileiro instituído pela Portaria Interministerial nº 3, de 08 de abril de 2015. Seu objetivo é “estimular o uso seguro e responsável das aplicações de internet e aplicativos, receber e encaminhar denúncias de crimes e violações de direitos humanos e promover um ambiente digital livre de discriminações” (art. 1º). Além da promoção de educação em direitos humanos e de segurança no uso das redes, por meio de materiais divulgados pela plataforma do #HumanizaRedes e de suas páginas em redes sociais, o programa se orienta a “enfrentar violações de direitos” por meio de canal online de recebimento de denúncias de violações de direitos humanos, ocorridas dentro e fora da Internet.

O programa é visto com reservas. O Projeto de Decreto Legislativo nº 47/2015<sup>56</sup> da Câmara dos Deputados, que ainda aguarda parecer da Comissão de Direitos Humanos e Minorias, por exemplo, pretende sustar a Portaria que instituiu o #HumanizaRedes, sob alegação, entre outras, de que ela não prevê critérios acerca de quais discursos serão considerados ofensas a direitos

<sup>54</sup> [https://www.wikileaks.org/spyfiles/files/0/31\\_200810-ISS-PRG-HACKINGTEAM.pdf](https://www.wikileaks.org/spyfiles/files/0/31_200810-ISS-PRG-HACKINGTEAM.pdf)

<sup>55</sup> <http://www1.folha.uol.com.br/poder/2015/04/1621459-pf-quer-instalar-virus-em-telefone-grampeado-para-copiar-informacoes.shtml>

<sup>56</sup> Fundamentação em <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=1214850>. Acessado em 17.06.15.

humanos<sup>57</sup> e, nesse sentido, por extrapolar os poderes do Executivo, já que a este não caberia definir quais seriam conteúdos ofensivos. A principal preocupação em termos de vigilância que a iniciativa desperta é, contudo, o fato de que incluirá uso de software, a ser desenvolvido em parceria com o Laboratório de Imagem e Cibercultura da Universidade Federal do Espírito Santo, que coletará dados de redes sociais a partir de temáticas pré-definidas pela Secretaria de Direitos Humanos e cartografará violações de direitos humanos na rede.<sup>58</sup> Não há previsões normativas formais sobre o funcionamento do programa, apenas esclarecimentos obtidos por meio da Lei de Acesso à Informação pela ONG Artigo 19.<sup>59</sup> Nelas, a Secretaria de Direitos Humanos afirma que a operacionalidade do software, sua metodologia e abrangência, assim como as temáticas pelas quais se guiará, ainda estão sob discussão no âmbito de grupo de trabalho responsável.

Vale notar que, em princípio, o #HumanizaRedes lida apenas com informações disponíveis publicamente na Internet, isto é, aquelas acessíveis por quaisquer usuários, em perfis públicos ou blogs, por exemplo. Por essa razão, ele não se caracteriza como uma forma típica de vigilância do Estado sobre as comunicações que, via de regra, se dão de forma privada. Apesar disso, seja pela plataforma de denúncia que cria ou pelo software de monitoramento do qual fará uso, o programa pode ter repercussões para a livre manifestação de pensamento, garantida pelo art. 5, inciso IV, da Constituição Federal, na medida em que pode interferir na liberdade dos cidadãos para postar conteúdos em seus perfis públicos na Internet.

## **RONDAS VIRTUAIS: A POLÍCIA NO FACEBOOK – CONTRIBUIÇÃO DA ARTIGO 19 E DA OFICINA ANTIVIGILÂNCIA**

Durante 2013 e 2014, diversos foram os critérios que os policiais usaram para definir quais seriam os sujeitos alvo de suas investigações no contexto das grandes manifestações públicas ocorridas no período.<sup>60</sup>

O inquérito policial que levou a prisão ou perseguição de mais de 20 manifestantes no Rio de Janeiro, por exemplo, revela que grande parte da investigação foi feita através do monitoramento das redes sociais e que os argumentos oferecidos para apresentar uma pessoa como suspeita eram baseados, muitas vezes, em comentários, fotos, tags e redes de amizade do Facebook<sup>61</sup>.

As denúncias e as intimações feitas no âmbito do inquérito eram respaldadas por informações coletadas nas chamadas "Rondas Virtuais"<sup>62</sup>, em que a polícia fazia uma varredura e analisava não só os perfis pessoais das pessoas consideradas suspeitas, mas também de parentes, amigos e

<sup>57</sup> O Grupo de Trabalho que gere o #HumanizaRedes foi criado pela Portaria Interministerial n. 2 de 20 de novembro de 2014. Ele tem a "finalidade de receber denúncias de manifestações nas redes sociais on-line de páginas e grupos de apologia ou promoção de crimes contra os direitos humanos, especialmente que incentivem a violência discriminante" (caput do art. 1º). Pelo parágrafo único do art. 1º, considera-se apologia ou promoção de crimes contra os direitos humanos toda manifestação que incentive a prática de qualquer um dos crimes previstos na Lei nº 7.716, de 5 de janeiro de 1989 ou no art. 140, § 3º do Código Penal." O escopo da atuação do #HumanizaRedes se refere, portanto a essa definição.

<sup>58</sup> GOVERNO FEDERAL DO BRASIL, "Governo vai usar software contra crimes de ódio na internet", publicada em 16.12.2014. Disponível em: <http://www.brasil.gov.br/cidadania-e-justica/2014/12/governo-vai-usar-software-contra-crimes-de-odio-na-internet> Acesso em 17.06.15.

<sup>59</sup> Pedidos e respostas à ARTIGO 19 estão disponíveis em: (i) <http://www.artigo19.org/centro/esferas/detail/706>; (ii) <http://www.artigo19.org/centro/esferas/detail/701> e (iii) <http://www.artigo19.org/centro/esferas/detail/702>, acessadas em 17.06.15.

<sup>60</sup> Sobre manifestações, ler mais em <http://www.artigo19.org/protestos/>.

<sup>61</sup> A Agência Pública teve acesso ao inquérito e ressaltou esses aspectos nesta reportagem: <http://apublica.org/2015/05/um-presos-politico-no-brasil-democratico/>

<sup>62</sup> "Ronda Virtual" é basicamente o trabalho manual de checar perfis de pessoas que estão associadas a páginas que apoiavam os protestos e eventualmente faziam apologia à depredação de patrimônio, contra policiais, etc. A prática já foi apresentada em outros casos em que a polícia se manifestou (e.g. <http://oglobo.globo.com/sociedade/oab-rj-aciona-ministerio-publico-estadual-policia-civil-para-investigar-paginas-consideradas-racistas-13953005>).

amigas, ou meros contatos do Facebook que se ligavam a elas a partir de comentários, curtidas, ou marcações feitas em posts e fotos relacionadas aos temas das manifestações. A impressão que fica é a de que a maioria da informação reunida foi proveniente de perfis públicos e com baixo nível de privacidade e que teriam facilitado a busca dos policiais. Porém, pelas informações que se tem do inquérito, é impossível determinar se o método utilizado foi apenas esse ou se também se fez uso de perfis falsos, com solicitações de amizade a usuários investigados para analisar informações não públicas, prática que, inclusive, já foi publicamente combatida pelo Facebook<sup>63</sup>, e que é questionável no nosso ordenamento.

Além do monitoramento de dados disponíveis nas redes sociais, houve, na mesma investigação, o pedido de quebra de sigilo de dados cadastrais de ao menos 46 perfis, 1 grupo e 3 páginas do Facebook, nos seguintes termos: "(...) dados cadastrais contendo Logs de criação e acesso, com data, hora e referência horária, IP, e-mail principal e secundário, telefones de confirmação, bem como demais informações constantes no banco de dados (cartões de crédito, se o perfil administra alguma página etc) (...)". O pedido de quebra de sigilo telemático das comunicações feitas por mensagens privadas no Facebook também foi pedido, incluindo dados como "texto, imagens, arquivos de áudio, localização etc" (SIC), registrados a partir de março de 2013 até a "data de deferimento da medida".

Mesmo que, no contexto das Rondas Virtuais, o monitoramento fosse feito a partir de dados de acesso público, o uso desses dados pelo Estado é questionável a partir do momento que são utilizados para formar supostos "perfis criminais" e "embasar" inquéritos. Tal ato deve ser considerado à luz dos direitos humanos fundamentais e dos preceitos do Código de Processo Penal, já que trata-se de forma questionável de busca de novas provas, tendo em vista que o inquérito não conseguia revelar indícios suficientes para a acusação dos envolvidos. Um dos réus, por exemplo, não é citado por nenhum depoimento, mas está sendo acusado por estar em uma foto com outro acusado portanto uma suposta arma, que, na verdade, seria uma espada de brinquedo. Ademais, os pedidos de quebra de sigilo, principalmente os telemáticos, também devem ser analisados diante dos limites de necessidade e proporcionalidade.

## **"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.<sup>64</sup> 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. 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.

<sup>63</sup> <http://www.techtudo.com.br/noticias/noticia/2014/10/facebook-veta-uso-de-perfil-falso-pela-policia-apos-polemica-com-nomes.html>

<sup>64</sup> ESTADO DE SÃO PAULO, "Abin monta rede para monitorar internet", publicada em Disponível em: <http://sao-paulo.estadao.com.br/noticias/geral,abin-monta-rede-para-monitorar-internet,1044500> Acesso em: 17.06.15.



## 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. Cabem agora fazer recomendações. Para tanto, serão utilizados como referência os 13 Princípios Internacionais sobre a aplicação de Direitos Humanos à Vigilância das Comunicações.<sup>66</sup>

## 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 pra garantir que as proteções à privacidade prossigam lado à 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 pra 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.

**TRANSPARÊNCIA:** O governo tem a obrigação de tornar públicas informações suficientes pra 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 pra acessar todas as informações relevantes a respeito das ações do Estado.

<sup>66</sup> <https://pt.necessaryandproportionate.org/text>

**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 pra 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 pela 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.

## 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 a efetividade da proteção que esses direitos garantem na prática. 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<sup>67</sup>; atualmente, na Alemanha, fala-se em introduzir obrigações de guarda por 10 semanas<sup>68</sup>. 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 da 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 e preparar intervenções por amici curiae.**

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). Ação que contesta sua constitucionalidade enfrentará, 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. Diante disso, o julgamento da constitucionalidade dessa lei estabelecerá precedentes importantes sobre a proteção à privacidade e ao sigilo das comunicações no Brasil. Intervenção nesse processo é imprescindível. Até o momento,, ingressou como amicus curiae apenas Associação Nacional dos Delegados de Polícia Federal.

**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 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), 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.

<sup>67</sup> 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 03.08.15.

<sup>68</sup> Ver novo projeto de lei para reintrodução da guarda obrigatória de metadados gerados na utilização de serviços de telecomunicações, a ser visto como tentativa de formulação de lei "proporcional" nessa matéria, disponível em [http://www.bmjv.de/SharedDocs/Downloads/DE/pdfs/Gesetze/RegE\\_Hochstspeicherfrist.pdf?\\_\\_blob=publicationFile](http://www.bmjv.de/SharedDocs/Downloads/DE/pdfs/Gesetze/RegE_Hochstspeicherfrist.pdf?__blob=publicationFile) Acesso em 03.08.15. 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 23.04.2015, disponível em <http://www.internetlab.org.br/pt/opiniao/uma-nova-lei-de-retencao-de-dados-para-a-alemanha-dessa-vez-constitucional/> Acesso em 03.08.15.

## **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.

Apesar disso, o Marco Civil da Internet possui, ainda, questões relevantes em aberto: institui guarda de dados, mas não contém prazo máximo – após o qual os dados devam ser apagados – nem estabelece normas e padrões de segurança expressos para os dados guardados (o que ameaça a proporcionalidade dessa obrigação); não contém regras de notificação dos usuários cujos dados são acessados (em claro desacordo ao princípio da notificação); não é preciso quanto aos destinatários da obrigação de guarda de registros de acesso a aplicações (problema de legalidade). Isso importa que o processo de elaboração do regulamento do Marco Civil da Internet, que deve dispor sobre estes assuntos, deva ser acompanhado de perto e influenciado em seu teor.

Além 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.<sup>69</sup> Isso parece sugerir que (i) a investigação criminal no Brasil é fortemente dependente de quebras de sigilo de dados cadastrais e de metadados, na falta de infraestrutura e pessoal para utilização de métodos de investigação ou da deficiência dos existentes; e/ou (ii) a morosidade do sistema judiciário brasileiro tem sido contornada por autoridades envolvidas em atividades investigativas, por meio de pressão por alterações legislativas que facilitem o acesso a dados. Nos dois casos, perdem os direitos fundamentais ao sigilo das comunicações, à privacidade e à liberdade de expressão. A realização de estudos empíricos sobre práticas de requisição de dados cadastrais e de metadados, colhendo-se números sobre quantidades de pedidos e realizando-se entrevistas com agentes envolvidos, poderá indicar razões reais desse panorama e indicar caminhos para a sua solução, dando conta de todos os interesses em jogo.

Paralelamente, é imprescindível que dados do Sistema Nacional de Controle de Interceptações da Corregedoria Nacional de Justiça sejam (i) disponibilizados publicamente, sem necessidade de se recorrer à Lei de Acesso à Informação, o que teve de ser feito para se obter os números apresentados neste relatório; e (ii) 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. Ao lado disso, é necessário, para respeito ao princípio da transparência, que dados sobre interceptações recolhidos pelo Conselho Nacional do Ministério Público em sistema próprio sejam também disponibilizados publicamente.<sup>70</sup> O controle sobre as interceptações não pode ser exercido sem publicidade sobre seus números.

#### **8) 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.<sup>71</sup> Recomendação básica parece ser aqui prestar atenção nesses órgãos, exigindo transparência sobre a sua atuação, para que avaliações completar sobre eles possam ser feitas, e, assim, o escrutínio público seja possibilitado.

<sup>69</sup> 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 <http://www.senado.gov.br/atividade/materia/getPDF.asp?t=55354&tp=1>. Acesso em 31.07.15.

<sup>70</sup> O InternetLab também solicitou à Ouvidoria do Conselho Nacional do Ministério Público acesso a informações sobre interceptações coletadas pelo sistema CNMPlnd. O acesso foi, contudo, negado, por alegado vício formal e porque as "informações solicitadas estão gravadas por sigilo legal". Vale lembrar que os números são meras estatísticas e não permitem quaisquer revelações sobre casos concretos, o que coloca a alegada proteção por sigilo em questão. Ver pedido e resposta em <http://ouvidoria.cnmpl.gov.br/ticket.php?track=AD7GASR276&Refresh=40756>. Acesso em: 31.07.15.

<sup>71</sup> 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 FOLHA DE SÃO PAULO, "Ameaça de bomba na Copa mobilizou inteligência e deixou Dilma apreensiva", publicado em 14.06.16, 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 31.07.15.

Quando se diz neste relatório que a ABIN não faz interceptações, que é o que manda a lei, diz 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.

