lavits ****** 2017
5to Simposio Internacional LAVITS
Vigilancia, Democracia y Privacidad
en América Latina: Vulnerabilidades y resistencias

ISSN 2175-9596

O CONTO DO BAÚ DO TESOURO: A EXPANSÃO DA VIGILÂNCIA PELA EVOLUÇÃO E POPULARIZAÇÃO DE CELULARES NO BRASIL

El cuento del tesoro: la expansión de la vigilancia por la evolución y popularización de los teléfonos celulares en Brasil

The treasure trove's tale: the expansion of surveillance by the evolution and popularization of cell phones in Brazil

Dennys Antonialli[a]
Jacqueline de Souza Abreu[b]

[(a)] Diretor-Presidente do InternetLab. Professor de Direito Constitucional da Faculdade de Direito da Universidade de São Paulo. São Paulo, SP, Brasil. Email: dennys@internetlab.org.br.
[(b)] Coordenadora da área de Privacidade e Vigilância do InternetLab. Doutoranda na Faculdade de Direito da Universidade de São Paulo. São Paulo, SP, Brasil. Email: jacqueline@internetlab.org.br.

Resumo

Este artigo descreve as formas como a "revolução do smartphone" permitiu novas formas de vigilância no Brasil. Aborda a falta de correspondência entre a evolução do uso do telefone e a tecnologia do telefone celular e as proteções fornecidas às comunicações no direito brasileiro. Para isso, apresenta dados empíricos sobre a evolução e o uso das tecnologias telefônicas no Brasil e fornece uma visão geral das leis, práticas e jurisprudência de vigilância no país, mapeando os principais problemas e lacunas que surgiram envolvendo acesso a dados de e gerados por telefones celulares.
Palavras-chave: Vigilância; Direito; Celulares; Privacidade; Segurança.

Resumen

Este artículo describe las formas en que la "revolución de los smartphones" ha permitido nuevas formas de vigilancia en Brasil. Aborda la falta de correspondencia entre la evolución del uso del teléfono y de la tecnología de los teléfonos móviles y las protecciones brindadas a las comunicaciones según el derecho brasileño. Para ello, presenta datos empíricos sobre la evolución y el uso de las tecnologías telefónicas en Brasil y proporciona una visión general de las

leyes de vigilancia, las prácticas y la jurisprudencia en el país, trazando los principales problemas y lagunas que han surgido con el acceso a datos de dispositivos móviles.
Palabras clave: *Vigilancia; Derecho; Móviles; Privacidad; Seguridad.*

Abstract

This article describes the ways in which the "smartphone revolution" has enabled new forms of surveillance in Brazil. It addresses the mismatch between the evolution of telephone usage and mobile phone technology and the protections provided to communications under Brazilian law. In order to do so, it presents empirical data on the evolution and usage of telephone technologies in Brazil and provides an overview of surveillance law, practices and case law in the country, mapping out the main issues and loopholes that have arisen involving access to mobile phones data.
Keywords: *Surveillance; Law; Smartphones; Privacy; Security.*

INTRODUÇÃO

A chegada de telefones celulares foi certamente um avanço para as comunicações em tempo real. A independência de dispositivos fixos permitiu que as pessoas alcançassem e fossem alcançadas a qualquer momento, revolucionando a forma como interagem entre si. A capacidade de transportar dispositivos telefônicos a qualquer lugar também deu origem a uma série de diferentes usos e aplicações, transformando telefones celulares em objetos (muito) inteligentes; uma das características mais importantes da tecnologia do telefone móvel é a conectividade com a Internet.

Ao provocar uma transformação na forma como as pessoas se comunicam, possibilitando a substituição das chamadas telefônicas tradicionais por aplicações de mensagens instantâneas, e-mails e até chamadas de voz sobre IP habilitadas para web, os telefones celulares também se tornaram um tesouro de informações de comunicações, particularmente para autoridades de segurança pública. Além dos registros detalhados sobre quando, onde e por quanto tempo as comunicações ocorreram, essas novas formas de troca de informações também podem armazenar todo esse conteúdo e muito mais, como lista de contatos, fotos, notas, listas de leitura, histórico de páginas visitadas, dados de localização.

Dado que o acesso a dados de comunicações é uma estratégia de investigação bastante disseminada no Brasil, este artigo descreve as formas como a "revolução do *smartphone*" permitiu novas formas de vigilância no Brasil. Apesar de a Constituição Federal brasileira de 1988 garantir o sigilo das comunicações, ela inclui uma exceção para fins de investigação e processo penal, a qual foi

regulamentada na Lei de Interceptações (Lei 9.296/1996). Desde então, as circunstâncias em que esse acesso é concedido mudaram significativamente, muito em razão da evolução e popularização de celulares.

Beneficiando-se de doutrinas desatualizadas e avançando interpretações expansivas, algumas autoridades policiais e representantes do Ministério Público têm reivindicado que o acesso ao conteúdo de comunicações armazenadas e a metadados deva seguir regras muito menos estritas do que as da Lei de Intercepções. Essas reivindicações estão sendo frequentemente consideradas adequadas pelo Judiciário, estabelecendo precedentes influentes. Além disso, a "Operação Lava Jato", investigação nacional sobre o maior esquema de corrupção da história, proporcionou um impulso para narrativas que reforçam capacidades investigativas, consolidando uma expansão sistemática de prerrogativas de vigilância, particularmente para a obtenção de evidências armazenadas em dispositivos eletrônicos.

O trabalho aborda a falta de correspondência entre a popularização do serviço de telefonia e a evolução dos telefones celulares, de um lado, e as proteções fornecidas às comunicações e dados pela legislação brasileira, de outro. Para isso, apresentamos evidências empíricas sobre a evolução e uso dessas tecnologias no Brasil e fornecemos uma visão geral das leis, práticas e jurisprudência de vigilância no país, mapeando os principais problemas que surgiram envolvendo acesso a dados de telefonia móvel[1].

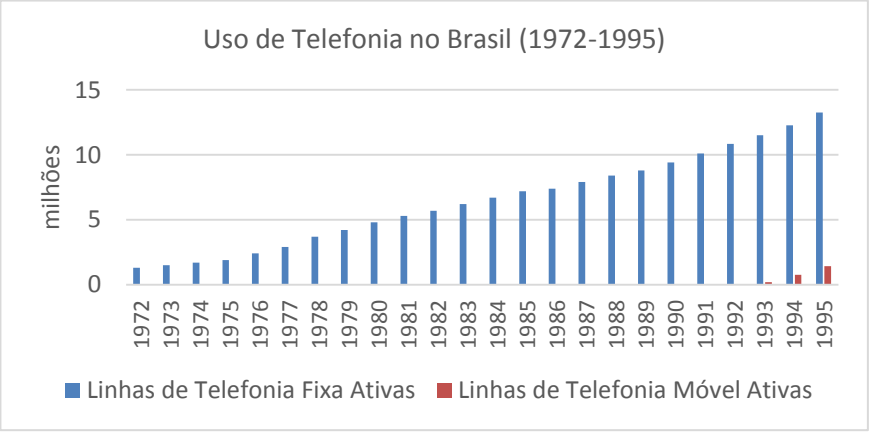
A REVOLUÇÃO DA TELEFONIA CELULAR NO BRASIL

A chegada do primeiro telefone no Brasil remonta ao final do século XIX, mas foi apenas nos anos 1950 que a indústria começou a florescer. No final dessa década, cerca de mil companhias telefônicas ofertavam serviços às áreas urbanas do país. Ainda passavam, entretanto, por desafios operacionais devido à falta de padronização e interoperabilidade. Para uma população de 70 milhões, não havia mais de 1 milhão de linhas telefônicas instaladas (Neves, 2002). De 1960 a 1996, o setor de telecomunicações viveu uma rígida intervenção do Estado. Mesmo assim, não experimentou a expansão em massa. Em 1995, havia apenas 13 milhões de celulares fixos no Brasil, agora com uma

[1] Este trabalho é um sumário dos resultados apresentados em (Abreu & Antonialli, 2017).

população de 162 milhões.

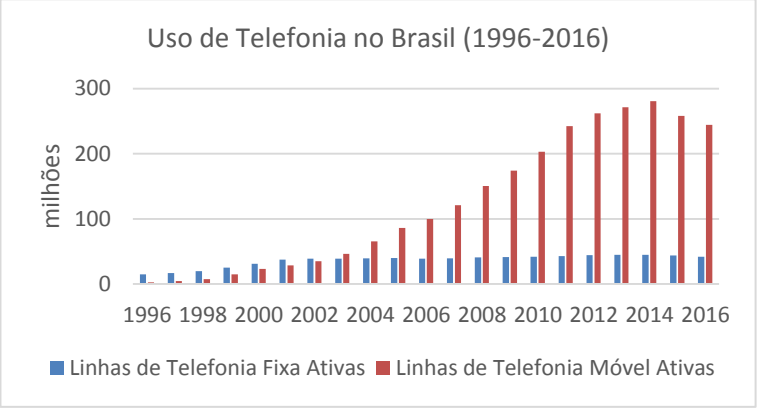
Figura 1



Agência Nacional de Telecomunicações: Gráfico - O uso de telefonia no Brasil (1972-1995). 2016.

Com a privatização do setor de telecomunicações em 1996, o objetivo da universalização dos serviços de telefonia ganhou fôlego. Para essa transformação, a introdução da tecnologia de telefonia móvel foi de extrema importância. A quantidade de assinaturas fixas ativas triplicou em 10 anos (13 milhões em 1995 para 39 milhões em 2005), mas desde 2010 estabilizou em cerca de 43 milhões. Por outro lado, a quantidade de assinaturas de telefones celulares aumentou dramaticamente, atingindo um pico de 280 milhões em 2014. A população brasileira era de 204 milhões no mesmo ano.

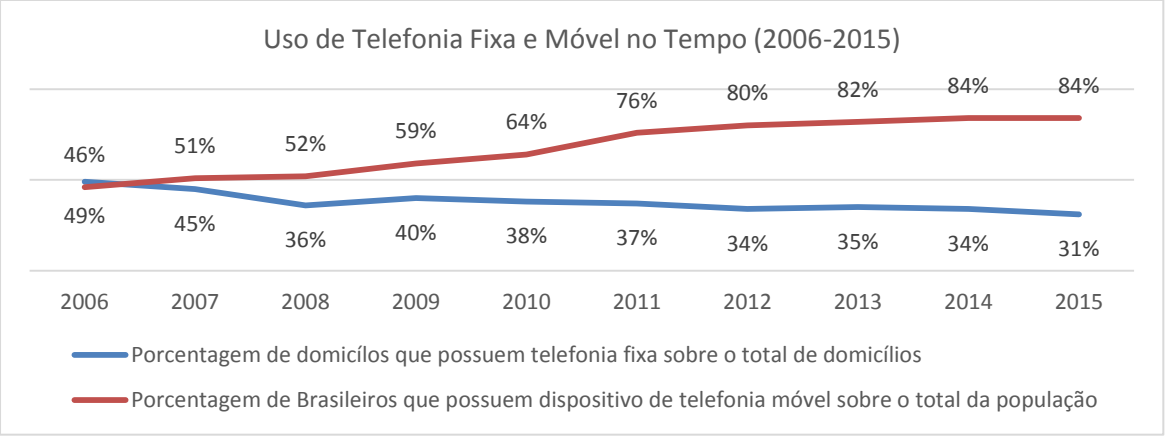
Figura 2



Agência Nacional de Telecomunicações: Gráfico - O uso de telefonia no Brasil (1996-2016). 2016.

Não só a grande maioria dos brasileiros (84%) agora possui telefones celulares, como também o número de telefones fixos está em declínio, confirmando que os celulares cresceram em importância como meio de comunicação (Figura 3).

Figura 3



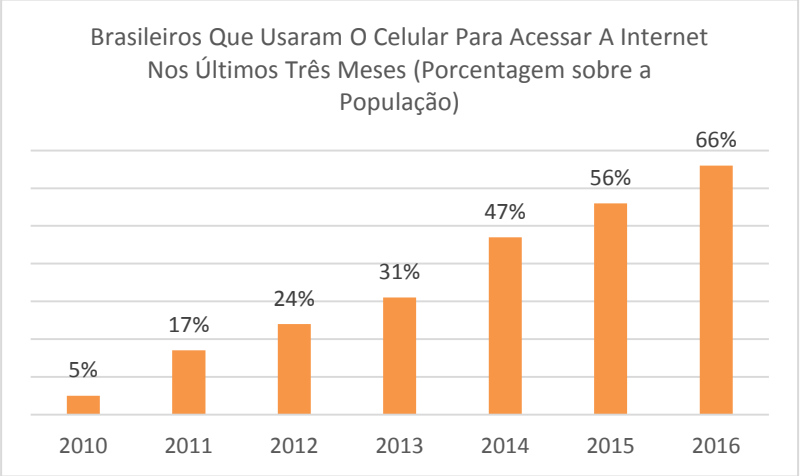
Comitê Gestor da Internet no Brasil: Uso de Telefonia Fixa e Móvel no Tempo (2006-2015). 2015.

Seguindo uma tendência global, no Brasil, os smartphones estão ganhando presença. Como os números abaixo mostram (Figura 4), a porcentagem de brasileiros que usam celulares para acessar a Internet - uma atividade típica do uso de smartphones – está crescendo rapidamente. Além disso, uma pesquisa IBOPE Inteligência de 2016, encomendada pela Qualcomm, indicou que a participação de brasileiros que possuem um smartphone passou de 19% em 2014 para 40% em 2016 (IBOPE Inteligência, 2016). Mais recentemente, uma pesquisa da Datafolha lançada no início de 2017, encomendada pela WhatsApp Inc., mostrou que 79% dos brasileiros adolescentes e adultos usam telefones inteligentes para acessar a Internet, atestando o crescimento da penetração desta tecnologia no Brasil (Datafolha, 2016).

Apesar dos números, vale a pena mencionar que a desigualdade social do Brasil também é atestada no uso da tecnologia de telefonia móvel. De acordo com uma pesquisa de 2015 do *think tank* estadunidense Pew Research Center, a proporção de brasileiros adultos que possuem um smartphone muda de acordo com o grupo demográfico (Poushter, 2016). Brasileiros mais jovens, mais educados e de classe superior, mais frequentemente, possuem smartphones. A título de exemplo, enquanto no grupo de renda mais alta 54% possuíam um smartphone, no grupo de baixa renda esse número caia

para 25%.

Figura 4



CETIC: Gráfico - Brasileiros Que Usaram O Celular Para Acessar A Internet Nos Últimos Três Meses (Porcentagem sobre a População). 2016.

A alta taxa de penetração da tecnologia de telefonia móvel no Brasil representa, em geral, um marco significativo, não só em termos de expansão do acesso à comunicação de longa distância, mas também a serviços baseados na Internet. Esses são números notáveis em termos de acesso ao conhecimento.

A proliferação de smartphones tem, no entanto, seu lado sombrio: expõe mais brasileiros a novas formas de vigilância, tanto do governo quanto do setor privado. Em termos de vigilância governamental, além das interceptações do conteúdo de comunicações em tempo real, o acesso a metadados e a informações armazenadas tornou-se uma prática comum, seja pela busca e apreensão de dispositivos ou pela devassa destes tipos de dados por meio de empresas de telecomunicações ou provedores de aplicações.

As ameaças decorridas dessas capacidades expandidas de vigilância seriam menos preocupantes se o direito brasileiro oferecesse aos seus cidadãos salvaguardas robustas em termos de proteção a direitos humanos que os resguardasse de acessos ilegais e abusivos aos seus dados.

Entretanto, como demonstramos na próxima seção, o direito brasileiro não avançou junto com os

dispositivos de telefonia móvel, deixando cidadãos – usuários de celulares – vulneráveis à vigilância ilegal e abusiva. A próxima seção oferece um quadro geral do regime legal aplicado e identifica as principais questões que surgem de interpretações ultrapassadas, vácuos, e medidas de controle insuficientes, típica e eficientemente exploradas por autoridades de segurança pública no Brasil.

O QUADRO NORMATIVO DA VIGILÂNCIA: AS QUESTÕES CENTRAIS

Apesar de a Constituição Federal brasileira de 1988 proteger o sigilo das comunicações e a privacidade, disputas interpretativas repercutem no grau de proteção que esses direitos garantem contra a vigilância indevida de autoridades do Estado sobre comunicações.

A primeira fragilidade decorre de uma persistente controvérsia sobre o âmbito de proteção conferido ao sigilo das comunicações, garantido no inciso XII do art. 5º ("XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal"). Dessa redação pouco clara surgem basicamente duas questões interpretativas principais: (i) qual é o objeto de proteção do sigilo: o *conteúdo* das informações comunicadas e transmitidas pelos meios citados (isto é, as correspondências, mensagens telegráficas, dados e telefonemas em si) ou o mero *fluxo* dessas informações por esses meios? (ii) qual(-is) grupo(-s), dentre os quatro listados no inciso, estão submetidos à exceção constitucional que permite a quebra do sigilo ("salvo, no último caso...")?

O entendimento doutrinário até hoje predominante (Ferraz, 1993; Ferreira, 2009; Silva, 2008), que também encontra eco em decisão do Supremo Tribunal Federal[2] (STF), é no sentido de que *(i)* a proteção do inciso XII do art. 5º não se refere ao conteúdo das informações comunicadas em correspondências, mensagens telegráficas, dados e telefonemas em si, mas sim à sua comunicação, isto é, ao seu *fluxo* enquanto ocorrem e que *(ii)* apenas o sigilo da comunicação por *telefonia*, enquanto está em fluxo, poderia ser restringido para fins de investigação criminal e instrução processual penal, não se estendendo essa possibilidade para o fluxo de dados, telegrafias e cartas.

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

Decorre dessa interpretação o entendimento de que estão excluídos do âmbito de proteção do dispositivo não somente o *conteúdo* de comunicações armazenadas, registradas ou gravadas como também as informações geradas a respeito das circunstâncias nas quais as comunicações ocorreram (metadados).

Além disso, o entendimento predominante é o de que somente comunicações telefônicas *em fluxo* poderiam ter seu sigilo afastado; essa possibilidade não se aplicaria a comunicações por correspondências, telegrafias e dados, enquanto em fluxo, os quais seriam absolutamente invioláveis. Tal interpretação, mesmo que ainda respaldada por parte da doutrina, não reflete a jurisprudência dos tribunais, que passou a admitir "quebras" do sigilo do fluxo das comunicações de todos os tipos, isto é, não só de comunicações telefônicas, desde que "proporcionais", quando se fundamentarem em direito fundamental conflitante ou em interesse público[3]. Também não reflete a atuação do Congresso Nacional que, em 1996, ao regulamentar a quebra de sigilo de comunicações telefônicas, como autoriza a Constituição Federal expressamente, também incluiu a possibilidade de se realizar interceptações "telemáticas" (o que abarca interceptações de "dados") na Lei de Interceptações. Em 2014, o Congresso também voltou a explicitamente admitir interceptações de comunicações eletrônicas (que, igualmente, envolvem "dados") no Marco Civil da Internet.

A partir da constituição, outras leis abordam questões específicas que envolvem o acesso a comunicações por parte de autoridades para fins de investigação criminal. Seja porque elas foram redigidas para um contexto tecnológico diferente ou porque adotaram linguagem ampla, essas leis contêm lacunas que foram e são exploradas por autoridades de segurança pública. Além disso, lacunas em tais textos deixam muitas questões abertas, expondo os usuários de celulares a uma vigilância ainda maior e mais invasiva. Nas subseções abaixo, resumimos as principais circunstâncias que contribuem para acentuar esse problema.

[3] No habeas corpus 70814/SP (Min. Rel. Celso de Mello, julg. em 01.03.2004), por exemplo, o Supremo Tribunal Federal admitiu que a administração penitenciária pode interceptar carta de preso, por razões de segurança pública, disciplina prisional ou preservação da ordem jurídica, com base no art. 41, parágrafo único, da Lei 7210/84, a lei de Execuções Penais, que restringe o direito do preso "ao contato com o mundo exterior por meio de correspondência escrita" (art. 41, XV, da mesma lei).

ACESSO A DISPOSITIVOS ELETRÔNICOS MEDIANTE MANDATOS DE BUSCA E APREENSÃO

A interpretação constitucional restritiva dada ao sigilo das comunicações, qual seja a de que ele só protegeria (conteúdo de) comunicações enquanto estão em *fluxo*, gera uma situação de descompasso normativo: os modernos celulares, *tablets* e computadores armazenam uma enorme quantidade de

informações, fotos e comunicações que oferecem retratos fieis e detalhados de seus donos, mas que não gozariam da mesma proteção de comunicações em fluxo pelo mero fato de agora estarem arquivadas.

A Lei das Interceptações (Lei nº 9.296), de 1996, surgiu para regular a hipótese de aplicação da exceção constitucional ao sigilo das comunicações, determinando as circunstâncias nas quais as autoridades do Estado podem ter acesso a comunicações telefônicas e telemáticas enquanto *em fluxo*, seja por meio da realização de interceptações junto a empresas de telefonia ou do emprego de grampos ou escutas ambientais. Para tanto, estabeleceu um regime jurídico rigoroso, que envolve o preenchimento de requisitos mais difíceis de ser atendidos. Esses requisitos estão previstos no art. 2º da lei e exigem *(i)* a configuração de indícios razoáveis da autoria ou participação em infração penal; *(ii)* a inexistência de outros meios de prova; e *(iii)* o envolvimento em crimes de maior gravidade. A lei estabeleceu também um limite temporal para realização dessa medida (15 dias, renováveis).

Diferente é a situação da proteção (a conteúdo) de comunicações armazenadas, isto é, as que não estão mais em trânsito. A legislação infraconstitucional toca a questão em duas leis diferentes. Quando o acesso a essas comunicações se dá por meio de um intermediário, que detém os dados (como é o caso de provedores de aplicações de Internet), os dispositivos aplicáveis são aqueles previstos no Marco Civil da Internet, o qual determina que o acesso ocorra mediante "ordem judicial" (art. 7º, III) nas hipóteses e na forma que a lei o estabelecer (art. 10, § 2º), sem, entretanto, explicitar requisitos substantivos de padrão probatório.

Quando o acesso se dá diretamente no aparelho apreendido, o regime não é claro. Não há regras específicas desenhadas e aplicadas para a busca de dispositivos *eletrônicos*, dando lugar a discricionariedade judicial, insegurança jurídica e abusos. Diante disso, pode-se dizer que, atualmente, comunicações armazenadas, registradas em celulares e computadores, provavelmente por

anos a fim, gozam de um grau de proteção menor do que comunicações em *fluxo*, cujo acesso se encontra regulamentado de forma mais rigorosa pela Lei de Interceptações.

Este paradoxo já começa a ser identificado e contestado em artigos de opinião (Antonialli, Cruz, & Valente, 2016; Maranhão, 2016). Na doutrina, também já começa a se argumentar que o art. 5º, XII da Constituição deveria garantir proteção irrestrita a *conteúdo* de comunicações, estejam elas em fluxo ou armazenadas, com a implicação de que toda quebra de sigilo de conteúdo deveria seguir os requisitos atuais da Lei das Interceptações (Sidi, 2015).

O Superior Tribunal de Justiça (STJ), em julgamento de setembro de 2016, já afastou essa tese. Na mesma decisão, afirmou a legalidade da prova obtida por celulares apreendidos no âmbito da Operação Lava Jato mediante mandado de busca e apreensão, mesmo sem autorização judicial específica que delimitasse a "busca virtual"[4]. No Recurso Extraordinário 418.416-8/SC, julgado em 2006, o Supremo Tribunal Federal também admitiu que o mero mandado de busca e apreensão já legitima acesso a dados armazenados em computadores.

Apesar de separadas por dez anos, as duas decisões demonstram quão penetrantes são as raízes do entendimento de que dados armazenados não estão protegidos pelo direito ao sigilo das comunicações na jurisprudência nacional, o qual alimenta o descompasso normativo entre a proteção de comunicações em fluxo e comunicações armazenadas.

ACESSO A DISPOSITIVOS ELETRÔNICOS APÓS PRISÃO EM FLAGRANTE

Um cenário igualmente problemático é o de quando o acesso a dados armazenados em dispositivos eletrônicos – principalmente celulares – se dá durante ou logo após uma prisão em flagrante. Quando autoridades policiais realizam prisões em flagrante, procedem à busca de objetos e produtos do crime portados pelo preso, para coleta de elementos que constituirão o auto de prisão em flagrante e também como medida de segurança das próprias autoridades. Nesse cenário, tem-se questionado se é permitido às autoridades policiais acessar também dados armazenados no celular portado pelo preso. A prisão em flagrante autoriza a devassa não só à pessoa em si e/ou ao seu domicílio, mas também a tudo que está salvo eletronicamente junto em dispositivos do preso? Outra vez a controvérsia sobre o

[4] SUPERIOR TRIBUNAL DE JUSTIÇA. Recurso em Habeas Corpus nº 75.800-PR. Ministro Felix Fischer, julgado em 15.09.2016. Disponível em: http://www.internetlab.org.br/wp-content/uploads/2016/11/lavajato.pdf.

regime de proteção de dados (conteúdo de comunicações e metadados) *armazenados* surge.

Não há convergência nos tribunais superiores acerca da legalidade desse acesso e das provas daí obtidas. Em julgado de 2012, o STF decidiu que a análise de registros telefônicos (metadados) de celular apreendido após prisão em flagrante não caracteriza violação ao sigilo das comunicações (art. 5, inciso XII), porque sua proteção abarcaria "comunicações de dados e não dados em si" e porque "comunicação telefônica e registros telefônicos recebem proteção jurídica distinta"[5]. Em 2007, o STJ já havia decidido de forma semelhante: a verificação de histórico de chamadas efetuadas e recebidas após prisão em flagrante não configura quebra ilegal de sigilo, porque as informações não foram obtidas por intermediário (empresas telefônicas) e nem se obteve conhecimento de conteúdo de conversas efetuadas.[6] Em 2016, por outro lado, agora lidando com um *smartphone* e demonstrando-se ciente da enorme quantidade de dados que um celular moderno produz e armazena, o STJ decidiu que a verificação de histórico de conversas do WhatsApp (conteúdo) em celular apreendido após flagrante constitui quebra de sigilo, isto é, é ilegal na falta de ordem judicial autorizadora[7].

Em tribunais estaduais, a apreciação do tema permanece casuística. Nos Tribunais de Justiça do Paraná[8], do Rio de Janeiro[9] e do Espírito Santo[10], foram encontrados julgados de 2016 que consideram que o acesso a dados de celular apreendido após flagrante prescinde de autorização judicial. A fundamentação utilizada é o art. 6º do Código de Processo Penal (CPP), o qual autoriza autoridades policiais a apreenderem objetos que tiverem relação com o fato delituoso e colherem todas as provas que servirem para o esclarecimento do fato e suas circunstâncias Essa posição também é encontrada na doutrina (Barreto & Férrer, 2016). No Tribunal de Justiça do Distrito Federal[11] e na Quarta Vara Federal Criminal em São Paulo[12] há decisões em favor da necessidade de autorização judicial, tendo em vista que o acesso a dados armazenados em celulares apreendidos constitui "busca virtual" e que celulares modernos deixaram de ser apenas instrumentos de

[5] SUPREMO TRIBUNAL FEDERAL. Habeas Corpus nº 91.867/SP. Min. rel. Gilmar Mendes, julg. 24.04.2012.
[6] SUPERIOR TRIBUNAL DE JUSTIÇA. Habeas Corpus nº 66.368/PA. Min. rel. Gilson Dipp, 5ª Turma, julg. 05.06.2007.
[7] SUPERIOR TRIBUNAL DE JUSTIÇA. Recurso Ordinário em Habeas Corpus nº 51.531/RO. Min. rel. Nefi Cordeiro. 6ª Turma, julg. 19.04.2016.
[8] TRIBUNAL DE JUSTIÇA DO PARANÁ. Habeas Corpus nº 1547585-9/PR. Rel. Maria José de Toledo Marcondes Teixeira. 5ª Câmara Criminal, julg. 14.07.2016.
[9] TRIBUNAL DE JUSTIÇA DO RIO DE JANEIRO. Apelação Criminal 01963693720158190001 RJ. Rel. Marcus Henrique Pinto Basílio, Primeira Câmara Criminal, julg. 17.05.2016.
[10] TRIBUNAL DE JUSTIÇA DO ESPÍRITO SANTO. Apelação Criminal 00070812320148080030. Rel. Sérgio Luiz Teixeira Gama, 2ª Câmara Criminal, julg. 24.02.2016.
[11] TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL E TERRITÓRIOS. Apelação Criminal 20150110776509 0023326-92.2015.8.07.0001. Rel. João Timóteo de Oliveira, 2ª Turma Criminal, julg. 03.11.2016.
[12] "Provas obtidas em celular de preso em flagrante são ilícitas". Consultor Jurídico. 26 de setembro de 2015, disponível em http://www.conjur.com.br/2015-set-26/provas-obtidas-celular-preso-flagrante-sao-ilicitas.

conversação de voz. Na Sétima Vara Federal Criminal em São Paulo, juiz considerou que prova obtida da verificação de mensagens de WhatsApp são ilegais; por outro lado, policiais estariam autorizados a consultar os últimos registros telefônicos para descobrir "comparsas"[13].

ACESSO A DADOS PROTEGIDOS POR CRIPTOGRAFIA DE PONTA-A-PONTA

O WhatsApp é o aplicativo de mensagens eletrônicas mais popular no país. Segundo uma pesquisa encomendada pela empresa, 9 entre 10 portadores de celular no Brasil usam o aplicativo (Datafolha, 2016). Principalmente após a implementação da criptografia de ponta-a-ponta pelo aplicativo em abril de 2016, o uso dessa tecnologia de proteção da confidencialidade de mensagens também se tornou motivo de controvérsia no Brasil. Isso porque a implementação dessa criptografia impossibilita a realização de interceptações telemáticas – a captura das conversas de alvos específicos em tempo real, mesmo mediante ordem judicial. Como a empresa também não armazena mensagens pretéritas em seus servidores, não é possível obter nenhum tipo de conteúdo de conversa com a empresa no âmbito de investigações. Tal obstáculo técnico esteve por trás de decisões de bloqueio contra o aplicativo (Abreu, 2016). Para os juízes envolvidos nesses casos, uma tecnologia que impede a realização de interceptações seria contrária à exceção prevista no inciso XII do art. 5º da Constituição Federal, que autorizaria o acesso a comunicações telefônicas em tempo real para fins de investigação criminal ou instrução processual penal. O STF, na Ação Direta de Inconstitucionalidade 5527 e na Arguição de Descumprimento de Preceito Fundamental 403, que analisam a compatibilidade de bloqueios do WhatsApp com a Constituição Federal, também foi instado a se manifestar sobre a o impasse (Abreu, 2017; Barros, 2016).

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

[13] Policiais causam anulação de provas por vasculharem WhatsApp sem autorização, 10 de março de 2017, disponível em http://www.conjur.com.br/2017-mar-10/policiais-vasculham-whatsapp-autorizacao-invalidam-provas.

constitucional da questão, vale também destacar que, atualmente, não há na legislação brasileira obrigação oponível aos desenvolvedores de aplicativos de mensagens no sentido de construírem a arquitetura de seus serviços de modo a permitir interceptações. Isso porque as obrigações previstas na Lei das Interceptações e em resoluções da ANATEL se destinam apenas a empresas de telefonia e provedores de conexão, mas não a provedores de aplicações de Internet (Abreu & Antonialli, 2016).

ACESSO A DADOS DETIDOS POR EMPRESAS DE TELEFONIA

Além de questões decorrentes da interpretação da constituição, as leis federais que regem a capacidade de vigilância do Estado para fins de aplicação da lei também apresentam problemas. A falta de clareza e salvaguardas e mecanismos de controle insuficientes expõem usuários de telefones celulares à vigilância abusiva.

Uma delas é a Lei das Organizações Criminosas (Lei Federal no. 12850/13), que conferiu a certas autoridades a prerrogativa de acessar dados cadastrais sem ordem judicial. O seu art. 15 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". Tal disposição repete o art. 17-B da Lei dos Crimes de Lavagem de Dinheiro (Lei nº 9.613/99), incluído pela Lei nº 12.683/2012.

Mesmo antes da sanção de tal previsão legal, autoridades policiais já defendiam a interpretação segundo a qual dados cadastrais não seriam resguardados pelos dispositivos constitucionais que protegem a privacidade e o sigilo das comunicações (art. 5, incisos X e XII), porque não se confundiriam com conteúdo de comunicações telefônicas. Em 2016, acolhendo tal posicionamento, o Tribunal Regional Federal da 3ª Região sustentou que a operadora Claro, que em 2013 impetrou mandado de segurança contra ofícios da Polícia Federal requisitando dados cadastrais de chips apreendidos, tem a obrigação de revelar dados de cadastro mesmo sem ordem judicial.[14]

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

Cabe ainda ressaltar que, apesar de a possibilidade de acesso a tais informações por mera requisição às empresas estar prevista nas leis sobre crimes de *organização criminosa* e de *lavagem de dinheiro*, as autoridades citadas pretendem também que o acesso por requisição não esteja limitado apenas a investigações e persecuções no âmbito de tais crimes, uma vez que o legislador não teria expressamente limitado tais competências apenas aos fins das leis em que se inserem (Aras, 2012). 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. A falta de quaisquer requisitos formais ou materiais para entregar a informação deixa esses procedimentos ainda mais discricionários.

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 e provedores de internet. O art. 17 obriga, entretanto, as companhias à guarda de "registros de identificação dos números dos terminais de origem e de destino das ligações telefônicas internacionais, interurbanas e locais" por 5 anos, os quais serão mantidos "à disposição das autoridades mencionadas no art. 15". O *caput* do art. 21, por sua vez, criminaliza a recusa ou omissão de "dados cadastrais, registros, documentos e informações requisitadas pelo juiz, Ministério Público ou delegado de polícia, no curso de investigação ou do processo", com pena de reclusão de 6 meses a 2 anos, e multa. Diante disso, tais autoridades têm requisitado, além dos dados cadastrais, registros telefônicos (e alguns até dados de localização), sem autorização judicial. Requisições diretas são feitas a empresas, sob ameaça de que serão punidas, caso não colaborem.

Ação Direta de Inconstitucionalidade (ADI 5063/DF, acima citada) foi proposta perante o Supremo Tribunal Federal contra tais artigos pela Associação Nacional de Operadoras Celulares (ACEL), sob

fundamento de violação ao direito à privacidade e ao princípio da legalidade, dada a insegurança jurídica acarretada pela imprecisão das normas[15]. A ação, proposta originalmente em 2013, ainda está pendente de julgamento.

ACESSO A DADOS DETIDOS POR PROVEDORES DE CONEXÃO E DE APLICAÇÕES DE INTERNET

Desenvolvido no contexto de um extenso debate público e promulgado em 2014, o Marco Civil da Internet (Lei Federal nº 12965/14) é de extrema importância na determinação da legalidade da vigilância estatal na Internet. Entre seus muitos princípios e regras, a lei desenvolve um regime claro de acesso a dados cadastrais, logs e conteúdo de comunicações. Lentamente, porém, encontraram-se maneiras de explorar lacunas e provisões ambíguas.

Ilustração disso são algumas decisões de tribunais estaduais que exigiram a retenção e determinaram a divulgação de informações relacionadas à "porta lógica de origem" por conexão e provedores de aplicações de internet (Cruz, 2016; Lopes, 2016; Blum, 2016) . Essa informação não faz parte das definições contidas na lei de "registros de conexão" e "registros de acesso a aplicação", que englobam apenas o endereço IP, data e hora. Afirmando que aquela é informação necessária para "identificar" os usuários – o "propósito" dos mandatos de retenção de dados –, a divulgação dessas informações foi confirmada pelos tribunais. De outro lado, o art. 10, § 3º, do Marco Civil da Internet ao menos 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.

[15] A petição da ACEL e exemplos de intimações recebidas por operadoras com base nessa (interpretação da) lei podem ser encontradas em CONJUR, "Operadoras reclamam de pedidos de delegados para quebra de sigilo telefônico", 29 de outubro de 2014, disponível http://www.conjur.com.br/2014-out-29/telefonicas-reclamam-quebras-sigilo-pedidas-delegados. Sobre a ação, ver notícia do site do STF, disponível em http://www.stf.jus.br/portal/cms/verNoticiaDetalhe.asp?idConteudo=254181.

Em termos de acesso a dados cadastrais, o Marco Civil 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, não há clareza sobre quem são essas 'autoridades administrativas' com poder de requerer diretamente dados cadastrais, o que permite que diversas autoridades governamentais reivindiquem essa prerrogativa para si.

Finalmente, a quebra de sigilo de conteúdo de comunicações eletrônicas em posse de provedores de aplicações de Internet (tais como Google e Facebook) está também prevista no Marco Civil da Internet, nos arts. 7º, III e 10, § 2º, os quais explicitam a necessidade de ordem judicial para tanto. Ao contrário do que ocorre para o fornecimento de registros (art. 22), entretanto, a lei não trata explicitamente dos requisitos formais e materiais que devem ser satisfeitos para que a ordem judicial seja concedida (Mendes & Pinheiro, 2015), o que dá margem a abusos e aplicações casuísticas.

ACESSO A DADOS DE LOCALIZAÇÃO

Não existe um regime geral de acesso a dados de localização no Brasil. Na prática, as autoridades de segurança pública reivindicam poderes de investigação gerais para fazer pedidos de dados de localização; somente se uma empresa se recusar a cumprir é que o assunto será submetido a um tribunal para revisão. Como a maioria das empresas desafia essas demandas quando não acompanhadas por uma autorização judicial, a proteção desse tipo de informação fica a critério de juízes.

Pelo menos dois exemplos ilustram quão vulnerável é a situação para usuários de telefonia móvel. Primeiro é o de uma decisão do 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[16]. Dado que não existe uma disposição legal nem jurisprudência que limita as violações da confidencialidade dos dados de localização aos casos criminais, e excluindo casos cíveis, esse acesso foi permitido.

O segundo exemplo está relacionado a um roubo a uma empresa de transportes de valores e de segurança em Ribeirão Preto em 2016. A polícia pediu judicialmente que que o Google, a Apple e a Microsoft fornecessem dados de todos os usuários que estiveram a até 500m do local do roubo, em um intervalo de 4 dias. A autoridade policial queria IMEIs (identificadores únicos dos aparelhos celulares), dados de usuário de contas de e-mail e os registros de acesso a elas, histórico de localização e deslocamento, histórico de buscas, senhas e fotos armazenadas na nuvem, tudo dos últimos 30 dias. O juiz de primeira instância concordou com parte do pedido e autorizou a quebra de sigilo dos dados cadastrais, dos lugares guardados no Google Maps e da localização e histórico de viagem dos últimos 30 dias de todos os usuários que estiveram nesses arredores por aqueles dias; o Google não acatou, e impetrou mandado de segurança no Tribunal de Justiça de São Paulo, mas apenas obteve uma redução do escopo do pedido; ainda não se conformando, levou o caso ao Superior Tribunal de Justiça. Só então, em uma liminar, o pedido foi revogado [17].

Os únicos parâmetros que existem em lei para o fornecimento de dados de localização foram adicionados ao CPP em dezembro e possuem aplicação bastante específica. O novo art. 13-B dispõe que "se necessário à prevenção e à repressão dos crimes relacionados ao tráfico de pessoas, o membro do Ministério Público ou o delegado de polícia poderão requisitar, mediante autorização judicial, às empresas prestadoras de serviço de telecomunicações e/ou telemática que disponibilizem imediatamente os meios técnicos adequados – como sinais, informações e outros – que permitam a localização da vítima ou dos suspeitos do delito em curso".

Nos detalhes, entretanto, a redação do dispositivo apresenta ambiguidades que podem dar margem a abusos, como por exemplo: *(i)* o *caput* do art. 13-B menciona "crimes relacionados a tráfico de pessoas", sem indicar expressamente a que tipos penais se refere; *(ii)* o mesmo artigo menciona

[16] 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.

[17] Superior Tribunal de Justiça. Pedido de Tutela Provisória nº 292-SP (2017-0034057-6), Min. Antonio Saldanha Palheiro, julg. 24 fev. 2017. Disponível em: http://www.internetlab.org.br/wp-content/uploads/2017/03/GooglevsMPSPnoSTJ_quebrageneralizadadesigilodelocalizacao.pdf.

também “meios técnicos” que permitam localizar pessoas: “sinais, informações e outros”; sem especificar quais seriam as “informações”, muito menos o que se deve entender por “outros”. De acordo com a definição genérica, vale tudo para localizar alguém – só não estaria diretamente incluída no pacote a quebra de sigilo de conteúdo de comunicações, que precisam de autorização específica (art. 13-B, § 2º, I). De acordo com o § 2º do art. 13-B, o “sinal” deve ser fornecido por período não superior a 30 dias (inciso II), renovável uma única vez por igual período. Em uma redação confusa, o inciso III do mesmo parágrafo afirma que “para prazos superiores, será necessária ordem judicial”, o que poderia dar lugar à interpretação de que não seria necessária a ordem para prazo inferior – ao contrário do que o caput requer.

Em janeiro de 2017, a Associação Nacional das Operadoras de Celular (ACEL) propôs ação direta de inconstitucionalidade (ADI 5642) contra esses dispositivos, por violarem os art. 5º, incisos X e XII da Constituição (Macedo & Coutinho, 2017).

CONCLUSÃO

A regulação de intercepções em tempo real de comunicações de longa distância e da instalação de grampos é um marco no regime legal de vigilância em muitos países. O Brasil não é uma exceção disso com sua Lei das Intercepções. No entanto, o uso da telefonia e dos próprios telefones mudou drasticamente desde a promulgação de tal legislação em 1996.

Os telefones celulares, de propriedade da grande maioria dos cidadãos brasileiros, são hoje um tesouro de informações de comunicação e, portanto, de evidências valiosas para agentes de segurança pública. Eles não são usados mais apenas para ligar. Eles armazenam enormes quantidades de informações pessoais que produzimos voluntariamente (nossos textos, fotos, notas, músicas, lista de contatos, histórico de chamadas). Eles também permitem que seus titulares usem serviços de Internet através de aplicativos ou navegadores, que também produzem e armazenam dados no dispositivo ou em outros locais. Inadvertidamente para as pessoas, eles também estão constantemente gerando outros tipos de informação, como dados de localização, para seu próprio funcionamento.

O Brasil carece, entretanto, de um quadro forte que estabeleça limites para o acesso de autoridades de segurança pública ao conteúdo das comunicações e aos metadados armazenados de celulares. Isso

significa que, embora a "revolução do smartphone" represente um marco em termos de acesso ao conhecimento e às comunicações no Brasil, também expõe os cidadãos brasileiros - usuários de smartphones – a uma vigilância maior e mais invasiva devido a leis desatualizadas, lacunas e jurisprudência amigável à vigilância. Repensar este quadro jurídico é fundamental para salvaguardar as liberdades individuais e evitar o encolhimento do espaço cívico em uma sociedade conectada (por smartphones).

REFERÊNCIAS

Abreu, J. de S. (2016, outubro 17). *From Jurisdictional Battles to Crypto Wars:* Brazilian Courts v. WhatsApp. Recuperado em 30 de outubro de 2017 de http://jtl.columbia.edu/from-jurisdictional-battles-to-crypto-wars-brazilian-courts-v-whatsapp.

Abreu, J. de S. (2017, junho 26). *Public hearing on encryption and WhatsApp blockages:* the arguments before the STF. Recuperado em 08 de agosto de 2017 de http://bloqueios.info/en/public-hearing-on-encryption-and-whatsapp-blockages-the-arguments-before-the-stf.

Abreu, J. de S., & Antonialli, D. (2016, julho 7). *State Surveillance of Communications in Brazil FAQ*. Recuperado em 08 de agosto de 2017 de https://necessaryandproportionate.org/state-surveillance-communications-brazil-faq.

Abreu, J. de S., & Antonialli, D. (2017). *Vigilância sobre as comunicações no Brasil:* interceptações, quebras de sigilo, infiltrações e seus limites constitucionais. São Paulo: InternetLab. Recuperado em 08 de agosto de 2017 de http://www.internetlab.org.br/wp-content/uploads/2017/05/Vigilancia_sobre_as_comunicacoes_no_Brasil_2017_InternetLab.pdf.

Agência Nacional de Telecomunicações (2016). *Relatório Anual ANATEL 2016*. Agência Nacional de Telecomunicações.

Antonialli, D., Cruz, F. B., & Valente, M. G. (2016, novembro 24). *Smartphones:* treasure chests of the Lava-Jato investigation. Recuperado em 08 de agosto de 2017 de http://www.internetlab.org.br/en/opinion/smartphones-treasure-chests-of-the-lava-jato-investigation.

Aras, V. (2012). A investigação criminal na nova lei de lavagem de dinheiro. *Boletim IBCCRIM, 237*. Recuperado em 08 de agosto de 2017 de https://www.ibccrim.org.br/boletim_artigo/4671-A-investigao-criminal-na-nova-lei-de-lavagem-de-dinheiro.

Barreto, A. G., & Férrer, E. F. de A. (2016). Perícia em celular: necessidade de autorização judicial? *Direito & TI*. Recuperado em 08 de agosto de 2017 de http://direitoeti.com.br/artigos/pericia-em-celular-necessidade-de-autorizacao-judicial.

Barros, P. P. (2016, novembro 21). *ADPF 403 in STF:* Are WhatsApp Blockings Constitutional? Recuperado em 08 de agosto de 2017 de http://bloqueios.info/en/adpf-403-in-stf-are-whatsapp-blockings-constitutional.

Blum, R. O. (2016, outubro 26). *Portas Lógicas de Origem*: identificação e caos jurídico. Recuperado em 08 de agosto de 2017 de http://jota.info/artigos/direito-digital-portas-logicas-de-origem-dificuldade-de-identificacao-e-o-caos-juridico-26102016.

Comitê Gestor da Internet no Brasil (2011). *TIC Domicílios e Empresas 2010* - Pesquisa sobre o uso das tecnologias de informação e comunicação no Brasil. São Paulo: Comitê Gestor da Internet no Brasil. Recuperado em 08 de agosto de 2017 de http://www.cetic.br/media/docs/publicacoes/2/tic-domicilios-e-empresas-2010.pdf.

Comitê Gestor da Internet no Brasil (2012). *TIC Domicílios e Empresas 2011* - Pesquisa sobre o uso das tecnologias de informação e comunicação no Brasil. São Paulo: Comitê Gestor da Internet no Brasil. Recuperado em 08 de agosto de 2017 de http://www.cetic.br/media/docs/publicacoes/2/tic-domicilios-e-empresas-2011.pdf

Comitê Gestor da Internet no Brasil (2013). *TIC Domicílios e Empresas 2012* - Pesquisa sobre o uso das tecnologias de informação e comunicação no Brasil. São Paulo: Comitê Gestor da Internet no Brasil. Recuperado em 08 de agosto de 2017 de http://www.cetic.br/media/docs/publicacoes/2/tic-domicilios-e-empresas-2012.pdf.

Comitê Gestor da Internet no Brasil (2014). *TIC Domicílios e Empresas 2013* - Pesquisa sobre o uso das tecnologias de informação e comunicação no Brasil. São Paulo: Comitê Gestor da Internet no Brasil. Recuperado em 08 de agosto de 2017 de http://www.cetic.br/media/docs/publicacoes/2/TIC_DOM_EMP_2013_livro_eletronico.pdf.

Comitê Gestor da Internet no Brasil (2015). *TIC Domicílios e Empresas 2014* - Pesquisa sobre o uso das tecnologias de informação e comunicação no Brasil. São Paulo: Comitê Gestor da Internet no Brasil. Recuperado em 08 de agosto de 2017 de http://www.cetic.br/media/docs/publicacoes/2/TIC_Domicilios_2014_livro_eletronico.pdf.

Comitê Gestor da Internet no Brasil (2016). *TIC Domicílios e Empresas 2015* - Pesquisa sobre o uso das tecnologias de informação e comunicação no Brasil. São Paulo: Comitê Gestor da Internet no Brasil. Recuperado em 08 de agosto de 2017 de http://www.cetic.br/media/docs/publicacoes/2/TIC_Domicilios_2014_livro_eletronico.pdf.

Cruz, F. (2016, junho 01). *Comentário, Porta Lógica e provedores de aplicação.* Recuperado em 08 de agosto de 2017 de http://omci.org.br/jurisprudencia/99/porta-logica-e-provedores-de-aplicacao.

Datafolha (2016). *Hábitos de Uso de Aplicativos, População brasileira, 13 anos ou mais*. Recuperado em 08 de agosto de 2017 de http://media.folha.uol.com.br/datafolha/2017/01/27/da39a3ee5e6b4b0d3255bfef95601890afd80709.pdf.

Ferraz, T. S. (1993). Sigilo de Dados: o direito à privacidade and os limites da função fiscalizadora do Estado. *Revista Da Faculdade de Direito Da Universidade de São Paulo, 88*, 439–459.

Ferreira, M. G. (2009). *Curso de Direito Constitucional* [35. ed.]. São Paulo: Saraiva.

Lopes, M. F. (2016, dezembro 17). E*ntrave tecnológico provoca impasse sobre o Marco Civil e anonimato*. Recuperado em 08 de agosto de 2017 de http://www.conjur.com.br/2016-dez-17/entrave-tecnologico-provoca-impasse-marco-civil-anonimato.

Macedo, F., & Coutinho. (2017, janeiro 25). Operadoras de celular vão ao Supremo contra lei que obriga repasse de dados a delegados e promotores. *O Estado de São Paulo*. Recuperado em 08 de agosto de 2017 de http://politica.estadao.com.br/blogs/fausto-macedo/operadoras-de-celular-vao-ao-supremo-contra-lei-que-obriga-repasse-de-dados-a-delegados-e-promotores/.

Maranhão, J. (2016, maio 12). O acesso ao WhatsApp pela operação Lava Jato. Recuperado em 08 de agosto de 2017 de http://jota.info/artigos/o-acesso-ao-whatsapp-pela-operacao-lava-jato-05122016.

Mendes, G. F., & Pinheiro, J. B. (2015). Interceptações e privacidade: novas tecnologias e a Constituição. In G. F. Mendes & I. W. Sarlet (Eds.), *Direito, Inovação e Tecnologia* (Vol. 1). São Paulo: Saraiva.

Sidi, R. (2015). A interceptação de e-mails e a apreensão física de e-mails armazenados. *Revista Fórum de Ciências Criminais*, *4*, 101–121.

Silva, J. A. (2008). *Curso de Direito Constitucional Positivo* (32nd ed.). São Paulo: Malheiros Editores.