A RESISTÊNCIA DOS PROVEDORES DE APLICAÇÕES DE INTERNET NO FORNECIMENTO DE ALGUMAS INFORMAÇÕES RELEVANTES À INVESTIGAÇÃO CRIMINAL

THE RESISTANCE OF INTERNET APPLICATION PROVIDERS IN THE PROVISION OF SOME INFORMATION RELEVANT TO CRIMINAL INVESTIGATION

LA RESISTENCIA DE PROVEEDORES DE APLICACIONES DE INTERNET EN OFRECER INFORMACIONES RELEVANTES PARA LA INVESTIGACIÓN CRIMINAL

Maurício Chouity Imay[1]
Flúvio Cardinelle Oliveira Garcia[2]

Resumo

A popularização da Internet de alta velocidade e os dispositivos portáteis de acesso a ela trouxeram inúmeros benefícios à sociedade mundial nas últimas décadas. Tal desenvolvimento tecnológico favoreceu o surgimento de sites e aplicativos que permitem a troca instantânea de mensagens, o uso de redes sociais, compartilhamento de arquivos eletrônicos diversos e muitas facilidades aos usuários. Entretanto, com esse desenvolvimento tecnológico também surgiram novos tipos de percalços, especialmente no que tange à investigação policial de crimes perpetrados através da Internet e aplicativos que a utilizam. Para a elucidação desses crimes, é frequente que as autoridades estatais necessitem de informações detidas somente pelas empresas que desenvolvem tais sites e aplicativos. O fornecimento de algumas dessas informações, mesmo diante de ordem judicial, algumas vezes é negado pelas empresas em tela. Nesse contexto, o presente trabalho tem como objetivo analisar a resistência de alguns provedores de aplicações de Internet que atuam no Brasil em fornecer informações relevantes à investigação criminal, verificar e comparar os dispositivos legais existentes, jurisprudências e atividades práticas da polícia judiciária.

Palavras-chave: Crimes cibernéticos. Provedor de aplicação. Investigação criminal.

Abstract

The popularization of high-speed Internet and portable Internet access devices has brought countless benefits to world society in recent decades. Such technological development allowed the emergence of websites and applications that allow the instant exchange of messages, the use of social networks, sharing of diverse electronic files, and numerous facilities for users. However, with this technological development, new types of mishaps have also arisen, especially concerning police investigation of crimes perpetrated through the Internet and applications that use it. To elucidate these crimes, state authorities frequently require information held only by the companies that develop such sites and applications. The provision of some of this information, even in the face of a court order, is sometimes denied by the companies on screen. In this context, the present study aims to analyze the resistance of some Internet application providers that operate in Brazil to provide some information relevant to a criminal investigation, verifying and comparing existing legal provisions, jurisprudence, and practical activities of the judicial police.

Keywords: Cybercrimes. Application provider. Criminal investigation.

Resumen

[1] Graduado em Engenharia Elétrica com ênfase em Eletrônica e Telecomunicações pela UTFPR. Especialista em Engenharia de Segurança do Trabalho pela UTFPR. Investigador de Polícia do Núcleo de Combate aos Cibercrimes – NUCIBER da Polícia Civil do Paraná. Graduado em Direito pela UNINTER. E-mail: mauricio.imay@gmail.com.
[2] Graduado em Ciências da Computação pela Universidade Católica de Brasília. Graduado em Direito pelo Centro Universitário de Brasília. Mestre em Direito Processual Penal pela Pontifícia Universidade Católica de São Paulo. Doutorando pela PUC/PR. Delegado de Polícia Federal. E-mail: fluvio.garcia@pucpr.br.

La popularización de la Internet de alta velocidad y los dispositivos portátiles de acceso a ella trajeron innúmeros beneficios a la sociedad mundial en las últimas décadas. Tal desarrollo tecnológico favoreció la aparición de páginas web y aplicaciones que posibilitan el intercambio instantáneo de mensajes, el uso de redes sociales, el compartir archivos electrónicos de diversos tipos y muchas facilidades a los usuarios. Sin embargo, con ese desarrollo tecnológico también se produjeron nuevos tipos de problemas, especialmente en lo que se refiere a la investigación policíaca de crímenes perpetrados por medio de la Internet y de aplicaciones que las utilizan. Para dilucidar esos crímenes, con frecuencia las autoridades estatales necesitan informaciones disponibles solamente en las empresas que desarrollan tales páginas y aplicaciones web. El suministro de algunas de esas informaciones, aun con orden judicial, a veces es negado por las empresas en cuestión. En ese contexto, el presente trabajo tiene el objetivo de analizar la resistencia de algunos proveedores de aplicaciones web que actúan en Brasil de suministrar informaciones relevantes para la investigación criminal, verificar y comparar las disposiciones legales existentes, la jurisprudencia y actividades prácticas de la policía judiciaria.

Palabras-clave: Crímenes cibernéticos. Proveedor de aplicación. Investigación criminal.

1 Introdução

O avanço da tecnologia e da Internet de alta velocidade trouxe inúmeras benesses à sociedade mundial, possibilitando, entre outros aspectos, maior facilidade de comunicação entre as pessoas, devido à popularização de dispositivos portáteis como os computadores pessoais e *smartphones*. Juntamente com o desenvolvimento desses dispositivos, surgiram sites de mídias sociais, aplicativos de troca de mensagens, lojas virtuais e diversas outras ferramentas que promovem a comunicação e interatividade entre pessoas e empresas, que se transformaram em uma alternativa à telefonia convencional, às reuniões presenciais e às lojas físicas, por exemplo. Entretanto, com esse avanço tecnológico, houve impactos relevantes no mundo jurídico, trazendo à tona a ocorrência de crimes perpetrados pela Internet ou por meios tecnológicos e que implicam na investigação policial desses delitos.

Nesse sentido, a necessidade de se obter informações detidas pelas empresas que desenvolvem tais programas e aplicativos mostra-se como caminho crítico para as investigações desempenhadas pela polícia judiciária no Brasil. A busca de uma prova ou de um dado que leve à autoria de determinado crime ocorrido na Internet ou por meio tecnológico pode estar somente de posse dos desenvolvedores do site, aplicativo ou ferramenta utilizada pelo criminoso. Logo, referida informação deveria ser provida às autoridades policiais, seja por meio de quebra de sigilo ordenada por juiz, seja mediante ofício da autoridade policial em determinadas situações. Ocorre que, em alguns casos, os detentores dessas informações, denominados provedores de aplicações de Internet, são resistentes em fornecê-las, mesmo diante de uma ordem judicial, contrariando o arcabouço jurídico pátrio.

Dessa maneira, este trabalho tem como problemática analisar a resistência de alguns provedores de aplicações de Internet que atuam no Brasil em fornecer informações relevantes à investigação criminal.

Para a elaboração deste artigo, foi realizada revisão bibliográfica, bem como a leitura e análise de artigos científicos e textos de assuntos correlatos ao tema. Foram também instrumentos de estudo a legislação vigente e jurisprudências. Para relatar a prática cotidiana enfrentada pelas autoridades policiais no que diz respeito ao tema estudado, foi realizada entrevista com um delegado de polícia que está à frente de uma unidade especializada no combate a cibercrimes. A experiência dos autores na atividade policial, em especial na investigação de cibercrimes, também contribuiu para o desenvolvimento deste trabalho.

2 Cibercrimes e investigação policial

Na década de 1990, quando a Internet se popularizou inicialmente no Brasil, sua utilização pelo usuário comum era vinculada a computadores pessoais (tipo PC – *Personal Computer*) equipados com placas *modem*[3], que se conectavam à rede mundial através de linha telefônica. Os sites da época, como o Altavista, Geocities, AOL, entre outros, eram estáticos e com pouca interação com o usuário, conforme aponta Scudere (2015, p. 2).

A popularização do computador pessoal e, principalmente, a portabilidade e a redução do custo de dispositivos que acessam a rede mundial, como os *smartphones*, nos levam ao que atualmente se chama de terceira onda da Internet, ou W*eb 3.0*, na qual os *sites* possuem algoritmos inteligentes, que se baseiam em comportamentos do usuário para apresentar resultados, conforme ensina Scudere (2015, p. 3). Também é pertinente que diversos objetos do cotidiano, antes tidos como autônomos, como simples eletrodomésticos, estão sendo desenvolvidos e comercializados para se conectarem à Internet, integrando o que se conhece por "Internet das coisas". Diante de tal cenário, existem milhões de desenvolvedores[4] de *websites* e aplicativos para os usuários desses dispositivos, seja um mero aplicativo para um telefone baseado no sistema *Android*[5] ou um site de relacionamentos sociais, como o *Facebook.*

Inúmeros são os crimes que podem ser cometidos através de meios eletrônicos, desde crimes contra a honra, falsidades, crimes contra o patrimônio, até aqueles que atentam contra a dignidade sexual, conforme lecionam Wendt e Jorge (2013, p. 20), na figura 1.

---

[3] Modems (modulador/demodulador) são equipamentos que transformam sinais digitais emitidos pelo computador em sinais analógicos que são enviados através de linhas telefônicas. Disponível em: http://understech.com.br/veja-como-funciona-modems-e-fax-modems/. Acesso em: 17 jun. 2018.

[4] Em outubro de 2016, existiam no mundo cerca de 12 milhões de desenvolvedores de aplicativos para dispositivos móveis, praticamente metade deles dedicados ao sistema Android, da Google. Disponível em: www.businessofapps.com/12-million-mobile-developers-worldwide-nearly-half-develop-android-first/. Acesso em: 17 jun. 2018.

[5] Em junho de 2017, a Google Store contava com cerca de 3 milhões de aplicativos. Disponível em: www.statista.com/statistics/266210/number-of-available-applications-in-the-google-play-store/. Acesso em: 17 jun. 2018.

Figura 1: Condutas indevidas praticadas através de computadores

CONDUTAS INDEVIDAS PRATICADAS POR COMPUTADOR		
AÇÕES PREJUDICIAIS ATÍPICAS	**CRIMES CIBERNÉTICOS ABERTOS**	**CRIMES EXCLUSIVAMENTE CIBERNÉTICOS**
✓ Invasão de computador sem o fim de obter, adulterar ou excluir dados e informações. ✓ Difusão de *phishing scam*	✓ Crimes contra a honra ✓ Ameaça ✓ Pornografia infantil ✓ Estelionato ✓ Furto mediante fraude ✓ Racismo ✓ Apologia ao crime ✓ Falsa identidade ✓ Concorrência desleal ✓ Tráfico de drogas	✓ Invasão de computador mediante violação de mecanismo de segurança com o fim de obter, adulterar ou excluir dados e informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita. ✓ Interceptação telemática ilegal ✓ Pornografia infantil por meio de sistema de informática ✓ Corrupção de menores em sala de bate papo ✓ Crimes contra a urna eletrônica

Fonte: Wendt e Jorge (2013, p. 20).

Diante da ocorrência de um crime cibernético, verificados os indícios de materialidade, as autoridades policiais buscam, por meio da investigação criminal, descobrir a autoria do delito e, normalmente, o criminoso vale-se do pseudoanonimato[6] proporcionado pela rede para praticar a ação, procurando dificultar sua localização e identificação pela polícia. Entretanto, Cerqueira e Rocha (2013, p. 145) apontam que qualquer atividade na Internet ocorre através de uma comunicação entre computadores, na qual é utilizado o protocolo de Internet (IP – *Internet Protocol*). Eleutério e Machado (2011, p. 106) explicam que, assim como as residências têm endereços, utilizados para receber correspondências, os computadores que fazem parte da Internet também necessitam de um endereço para receberem suas "correspondências digitais". Esse endereço é chamado de IP.

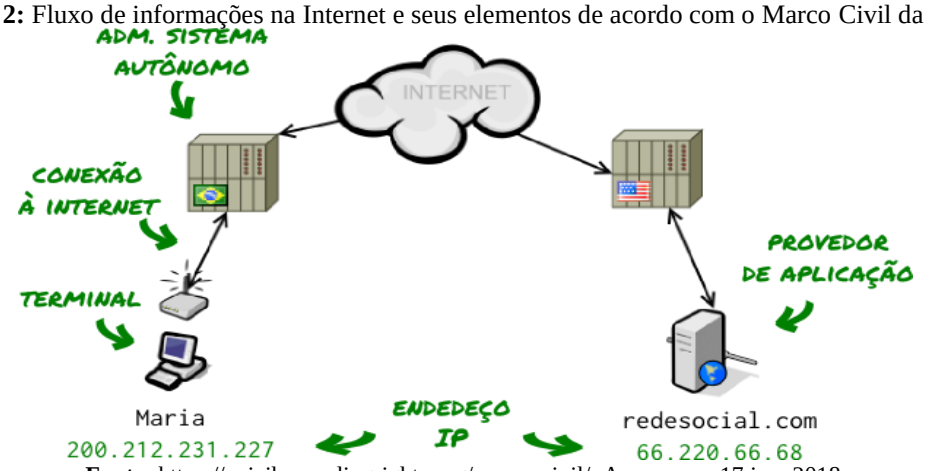
Uma vez que o autor do crime cibernético se vale do pseudoanonimato, a principal e mais sólida maneira de localizá-lo e identificá-lo é descobrindo o IP do qual partiu aquela ação criminosa, pois essa identificação leva à conexão de Internet utilizada pelo criminoso. Exemplificando: suponha que um criminoso utilizou o site de mídia social *Facebook*, através de um perfil fictício, para enviar uma mensagem que configure o crime de ameaça contra uma pessoa. Ao postar essa mensagem, o autor do crime utilizou um computador, de sua residência, com conexão à Internet[7] proporcionada através de um provedor de conexão

[6] "Grande parte dos acessos feitos de forma anônima usam a rede Tor, acrônimo para The Onion Router, um software livre e de código aberto que garante o anonimato pessoal ao navegar na Internet, protegendo os usuários contra a censura e também a sua privacidade pessoal. Atrelada a serviços de proxy, servidor que age como um intermediário para requisições de outros servidores, o Tor se torna uma ferramenta ainda mais importante". Disponível em: https://iq.intel.com.br/quao-anonimo-e-possivel-ser-na-internet-hoje/. Acesso em: 17 jun. 2018.

[7] "V - conexão à Internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela Internet, mediante a atribuição ou autenticação de um endereço IP". Art. 5º, V, Lei 12.965 de 23 de abril de 2014, Marco Civil da Internet.

(administrador de sistema autônomo[8] – uma operadora de telefonia, por exemplo), o qual atribuiu a esse computador um IP[9]. Através desse IP, o computador do criminoso acessou, transmitiu e recebeu dados dos servidores do *Facebook* (provedor de aplicação[10]). Toda essa ação, conforme bem lecionam Cerqueira e Rocha (2013, p. 153), gera registros no provedor de conexão[11] e registros no provedor de aplicação[12], seja registro do conteúdo da mensagem com a ameaça, sejam registros da data, horário e IP, seja registro de para qual cliente da operadora aquele IP está alocado naquele momento específico. Esse fluxo de informações na Internet e seus elementos são melhor ilustrados na figura 2.

Figura 2: Fluxo de informações na Internet e seus elementos de acordo com o Marco Civil da Internet



Fonte: https://cpiciber.codingrights.org/marco-civil/. Acesso em: 17 jun. 2018.

Diante disso, para se localizar e identificar o titular da conexão à Internet (pessoa física ou jurídica) da qual partiu a mensagem com a ameaça, a autoridade policial necessita das informações detidas pela operadora e pelo *Facebook*, a fim de estabelecer o vínculo entre a materialidade do crime e a autoria do mesmo.

Fica claro, portanto, e no diapasão do entendimento de Cerqueira e Rocha (2013, p. 153), que no centro de uma investigação criminal pautada na legalidade, as autoridades estatais necessitam da cooperação dos administradores de *websites* e aplicativos – os

[8] "IV - administrador de sistema autônomo: 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". Art. 5º, IV, Lei 12.965 de 23 de abril de 2014, Marco Civil da Internet.
[9] "III - endereço de protocolo de Internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais". Art. 5º, III, Lei 12.965 de 23 de abril de 2014, Marco Civil da Internet.
[10] "VII - aplicações de Internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à Internet". Art. 5º, VII, Lei 12.965 de 23 de abril de 2014, Marco Civil da Internet.
[11] "VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à Internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados". Art. 5º, VI, Lei 12.965 de 23 de abril de 2014, Marco Civil da Internet.
[12] "VIII - registros de acesso a aplicações de Internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de Internet a partir de um determinado endereço IP". Art. 5º, VIII, Lei 12.965 de 23 de abril de 2014, Marco Civil da Internet.

provedores de aplicação de Internet – e dos provedores de conexão para obter as informações que levem ao deslinde de uma investigação criminal. Obviamente, tal cooperação necessita ser regulamentada e controlada, sendo que, no ano de 2014, entrou em vigor a Lei nº 12.965, de 23 de abril de 2014, conhecida como Marco Civil da Internet. Tal diploma legal possui dispositivos que normatizam a mencionada cooperação entre provedores de aplicação e conexão e as autoridades estatais. Ademais, não se encontram dispositivos legais que disciplinam a matéria somente no Marco Civil da Internet, pois as Leis nº 9.296, de 24 de julho de 1996 (Lei de Interceptações Telefônicas); nº 9.613, de 3 de março de 1998 (Lei de Lavagem de Dinheiro), e nº 12.850, de 2 de agosto de 2013 (Lei de Combate ao Crime Organizado), possuem artigos relacionados à matéria em estudo.

Entretanto, mesmo com todo o arcabouço legal, a *práxis* demonstra que há inúmeras dificuldades na obtenção dessas informações que, conforme explanado, são de grande relevância para o esclarecimento de crimes, empecilhos estes causados, muitas vezes, por negativas dos provedores diante da requisição da autoridade policial ou ordem judicial, o que se caracteriza, portanto, como um claro desrespeito à norma legal. Com relação aos provedores de conexão à Internet, normalmente não ocorre a negação no fornecimento dos registros, pois são empresas sediadas e com infraestrutura de tecnologia em território nacional, que acatam a lei e as determinações judiciais. O que se vê na prática policial, também sustentado pelos autores Cerqueira e Rocha (2013, p. 153), é que os problemas em sua maioria ocorrem com os provedores de aplicações de Internet, os quais muitas vezes são empresas estrangeiras, que têm a sua infraestrutura de tecnologia – como computadores servidores, base de dados –, sediados em território estrangeiro, mas com representação no Brasil. Algumas dessas empresas descumprem alguns comandos judiciais, não fornecendo os registros.

Nesse diapasão, têm-se casos de notoriedade nacional, que foram os bloqueios do aplicativo de mensagens instantâneas *WhatsApp* em território brasileiro, ocorridos nos anos de 2015[13] e 2016[14]. Conforme esclarecem Barreto Junior e Lima (2016), tais bloqueios ocorreram por determinação judicial em primeiro grau, com o fundamento de que a empresa responsável pelo aplicativo negou-se a fornecer dados de suma importância para investigações policiais à época, que apuravam crimes envolvendo pornografia infantil, organizações

[13] "Já era! Justiça manda bloquear WhatsApp no Brasil imediatamente por 48h". Disponível em: https://www.tecmundo.com.br/whatsapp/91909-whatsapp-bloqueado-brasil-48h-justica-bloqueia.htm. Acesso em: 17 jun. 2018.

[14] "De novo! WhatsApp será bloqueado no Brasil a partir de hoje; entenda". Disponível em: https://www.tecmundo.com.br/whatsapp/104302-whatsapp-bloqueado-brasil-hoje-justica-entenda.htm. Acesso em: 17 jun. 2018.

criminosas e tráfico de drogas. Chama a atenção que nenhum dos bloqueios prosperou, pois após algumas horas sem atividade do aplicativo, decisões em âmbito recursal invalidaram ou reformaram as primeiras, desbloqueando a aplicação, conforme aponta Becker (2016). Alguns relatores arguiram que tais medidas seriam "desproporcionais", afetando "serviço essencial" de milhões de brasileiros[15]. Findou-se que, além dos bloqueios não terem surtido o efeito desejado, as autoridades solicitantes continuaram sem acesso aos dados relevantes para o esclarecimento das investigações criminais da época.

3 Internet e criminalidade

A Internet de alta velocidade proporcionou a popularização dos aplicativos de VOIP[16], *instant messaging*[17], lojas virtuais, mídias sociais, entre outros inúmeros aplicativos que fornecem facilidades aos usuários.

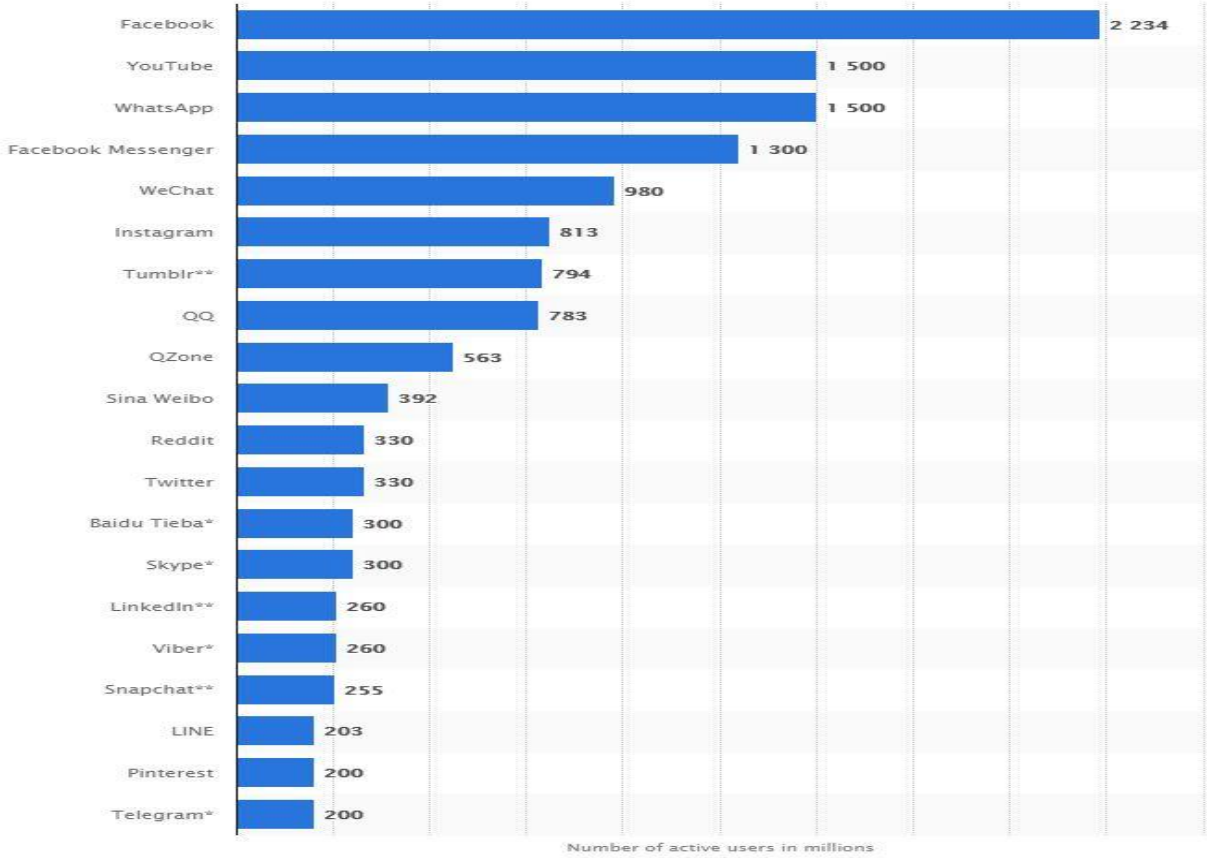
Nesse diapasão, pode-se observar na figura 3, dados coletados pelo *website* Statista, que informa as redes sociais e aplicativos mais famosos no mundo pela quantidade de usuários ativos, em abril de 2018.

[15] Tribunal de Justiça de Sergipe. Nº do processo: 201600110899 / 0003701-40.2016.8.25.0000 - Mandado de Segurança (Crime). Disponível em: http://www.tjse.jus.br/tjnet/jurisprudencia/relatorio.wsp?tmp_numprocesso=201600110899&tmp_numacordao=201616329&tmp.expressao=whatsapp. Acesso em: 17 jun. 2018.

[16] *Voice Over Internet Protocol*, ou voz sobre IP. É uma tecnologia que permite a transmissão de voz por IP (Protocolos de Internet), ou seja, transforma sinais de áudio analógicos, como em uma chamada, em dados digitais, que podem ser transferidos através da Internet.
Disponível em: http://www.techtudo.com.br/noticias/noticia/2015/03/entenda-o-voip-tecnologia-que-permite-apps-ligarem-pela-Internet.html. Acesso em: 17 jun. 2018.

[17] Mensageiro instantâneo. Os comunicadores instantâneos, também chamados de mensageiros instantâneos, são aplicativos que permitem o envio e recebimento de mensagens em tempo real. Disponível em: https://www.oficinadanet.com.br/post/14331-quais-sao-os-mais-famosos-mensageiros-instantaneos. Acesso em: 17 jun. 2018.

Figura 3: Redes sociais e aplicativos mais famosos no mundo pela quantidade de usuários ativos, em abril de 2018 (em milhões)



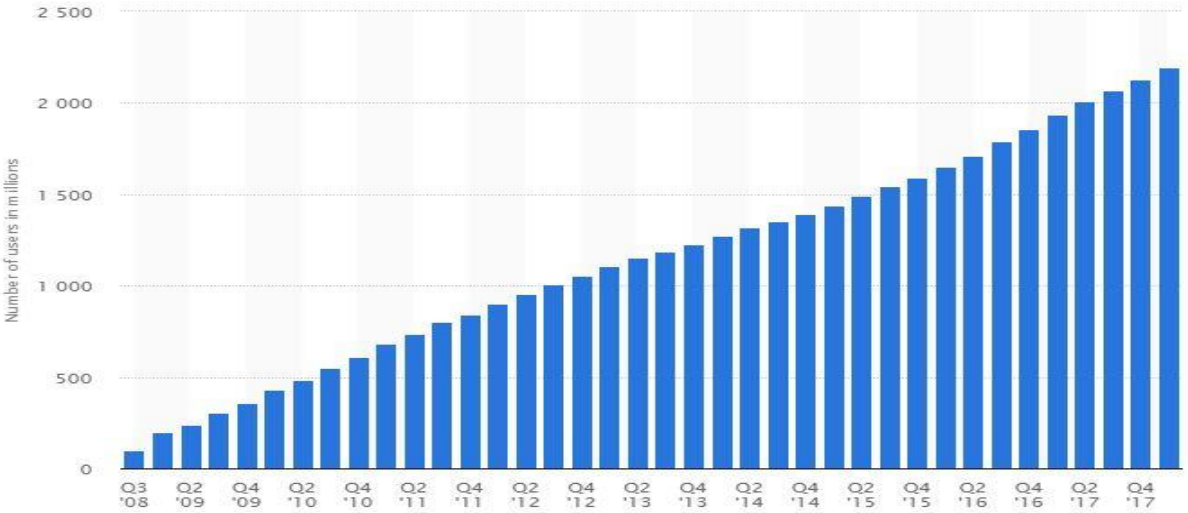
Fonte: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/. Acesso em: 17 jun. 2018.

Com isso, o número de crimes, sejam os exclusivamente cibernéticos[18] ou os que utilizam aplicativos de Internet como ferramenta no *iter criminis*, aumentou sobremaneira[19]. Logo, os meios tradicionais de investigação criminal utilizados pela polícia, que tinha como suprassumo a interceptação telefônica, não são mais tão efetivos e eficientes nesses casos. Exemplificando o problema: a interceptação telefônica de um traficante de drogas ou sequestrador há alguns anos era um excelente meio de prova na investigação e na ação penal. Atualmente, a popularização de aplicativos de *instant messaging*, como por exemplo, *WhatsApp*, Telegram, Viber, que possibilitam, além da troca instantânea de mensagens de texto, de áudio, imagens e outros tipos de arquivos e também a chamada de voz entre os usuários, tornou a interceptação telefônica tradicional, de certa maneira, menos eficiente.

[18] Crimes que somente podem ser praticados com a utilização de computadores ou de outros recursos tecnológicos que permitem o acesso à Internet, conforme Wendt e Jorge (2013, p. 19).

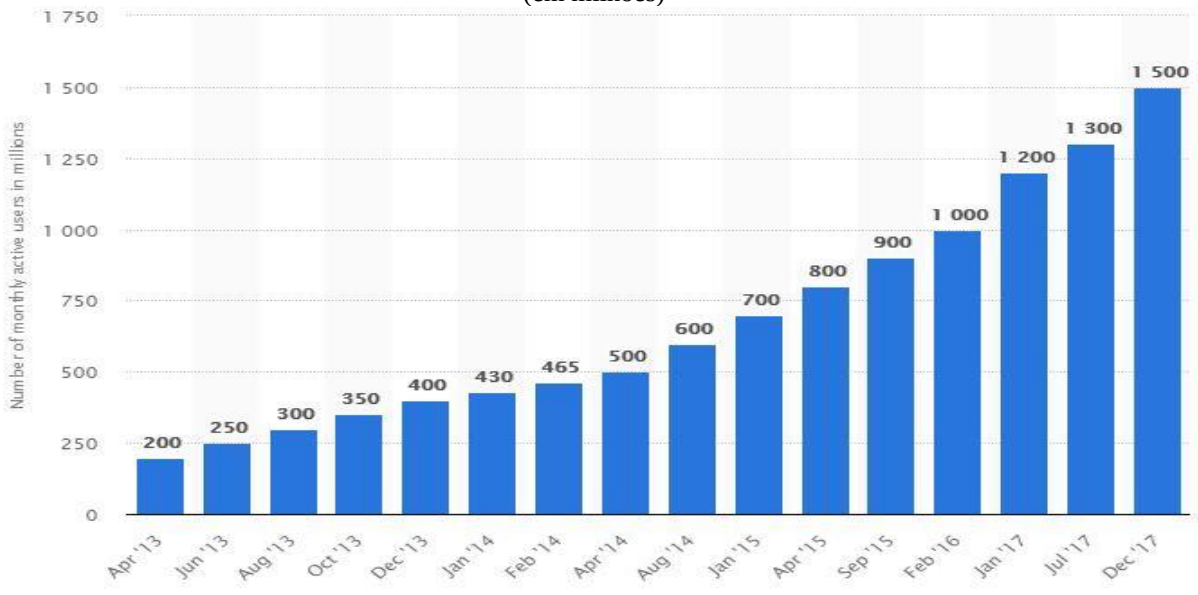
[19] "O Brasil ocupa lugar de destaque no cenário global de cibercrimes. Em 2016, 42,4 milhões de brasileiros foram vítimas de crimes virtuais. Em comparação com 2015, houve um aumento de 10% no número de ataques digitais. Segundo dados da Norton, provedora global de soluções de segurança cibernética, o prejuízo total da prática para o país foi de US$ 10,3 bilhões". Disponível em: http://economia.estadao.com.br/noticias/releases-ae,crimes-virtuais-afetam-42-milhoes-de-brasileiros,70001644185. Acesso em: 17 jun. 2018.

Figura 4: Número de usuários ativos do aplicativo *Facebook* no mundo até o primeiro trimestre de 2018 (em milhões)



Fonte: https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/. Acesso em: 17 jun. 2018.

Figura 5: Número de usuários ativos do aplicativo *WhatsApp* no mundo, de abril de 2013 a dezembro de 2017 (em milhões)



Fonte: https://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/ Acesso em: 17 jun. 2018.

Normalmente, ao se interceptar o telefone de um traficante, pouco se coleta de informações, pois o criminoso opta por utilizar aplicativos de VOIP e *instant messaging* para comunicar-se, em detrimento da telefonia convencional, pois sabe que as chances de ter sua conversa e localização descobertas são praticamente mínimas, provavelmente devido à propaganda que tais empresas fazem de seus aplicativos proporcionarem um ambiente de comunicação privado e seguro[20], através, por exemplo, da criptografia.

[20] Disponível em: https://www.whatsapp.com/security/. Acesso em: 17 jun. 2018.

Algumas informações, tais como registro de conexão (data, horário, fuso horário e IP) e alguns dados cadastrais são atualmente fornecidos pelas empresas mediante ordem judicial, porém são informações pretéritas, que podem demorar meses para alcançar os investigadores, tornando a apuração, em certos crimes, morosa, ineficaz e ineficiente, como é bem apontado por Cerqueira e Rocha (2013, p. 153). Entretanto, informações valiosas para o desvendamento mais célere de crimes (como a extorsão mediante sequestro, por exemplo), tais como a geolocalização do aparelho móvel em tempo real e o conteúdo das mensagens de aplicativos de *instant messaging* (mesmo as pretéritas), não são fornecidas às autoridades policiais brasileiras, mesmo diante de ordem judicial. Alguns provedores de aplicações são resistentes e não acatam ordens emanadas do Poder Judiciário brasileiro, pois alegam que ou não possuem tais dados armazenados, ou são tecnicamente impossíveis de serem obtidos ou que a lei estrangeira não permite fornecer tais dados sem a utilização de Acordos de Assistência Judiciária em Matéria Penal (*Mutual Legal Agreement Treaties* – MLATs). Domingos e Röder (2016, p.65), discorrem sobre o tema:

> Tais pedidos, conhecidos como Mutual Legal Agreement Treaties (MLATs) – Acordos de Assistência Mútua em Matéria Penal, tradicionalmente têm um processamento muito lento, pois dependem de que os pedidos sejam feitos de forma correta, de que sejam traduzidos e enviados pelas autoridades competentes, para que uma autoridade no país requerido dê início à execução do pedido.
> Esse procedimento protocolar, que já se apresentava por demais demorado para os pedidos tradicionais, é no mais das vezes inócuo face à volatilidade das provas digitais e da necessidade de investigação célere, não estando adequado às novas tecnologias.

Cerqueira e Rocha (2013) concluem que o resultado de tal omissão é a morosidade ou, em grande parte delas, o insucesso de investigações policiais de crimes que utilizam essas tecnologias para o seu cometimento pois, muitas vezes, essas informações são decisórias, estão no caminho crítico de uma investigação criminal.

Em investigações desencadeadas pelo Núcleo de Combate aos Cibercrimes – NUCIBER da Polícia Civil do Paraná, inúmeras são as solicitações da autoridade policial acerca de dados detidos pelos provedores de aplicações, com a finalidade única de obter êxito em investigações de crimes envolvendo pornografia com menores de idade, extorsões, estelionatos, furtos qualificados mediante fraudes, entre outros crimes de atribuição da mencionada unidade policial. Ocorre que, segundo o NUCIBER, mesmo após análise judicial, com consequente emanação de ordem, alguns provedores de aplicações, tais como, por exemplo, *Facebook* e Google, não acatam referidos expedientes judiciais no que tange a alguns dados em particular.

4 Fornecimento de informações pelos provedores de aplicação de internet às autoridades estatais no âmbito da investigação criminal

A investigação de delitos cometidos por meios tecnológicos que utilizam a Internet não é extremamente complexa, como muitos pensam. Wendt e Jorge (2013, p. 52, grifo nosso) explicam que o procedimento investigativo pode ser dividido em duas fases: fase técnica e fase de campo. Na fase técnica, os autores elencam as seguintes etapas:

> - análise das informações narradas pela vítima e compreensão do fato ocorrido na Internet;
> - orientações à vítima com o intuito de preservar o material comprobatório do delito e a sua proteção virtual;
> - coleta inicial de provas em ambiente virtual;
> - formalização do fato criminoso por intermédio de um registro ou boletim de ocorrência, com a consequente instauração do feito;
> - investigação inicial referente aos dados disponíveis na rede mundial de computadores sobre prováveis autores, origem de e-mails, registro e hospedagem de domínios;
> - formalização de relatório ou certidão das provas coletadas e apuração preliminar;
> - **representação perante o Poder Judiciário para expedição de autorização judicial para quebra de dados, conexão ou acesso. Também poderão ser solicitados os dados cadastrais para os provedores de conteúdo**.
> - análise das informações prestadas pelos provedores de conexão e/ou provedores de conteúdo.

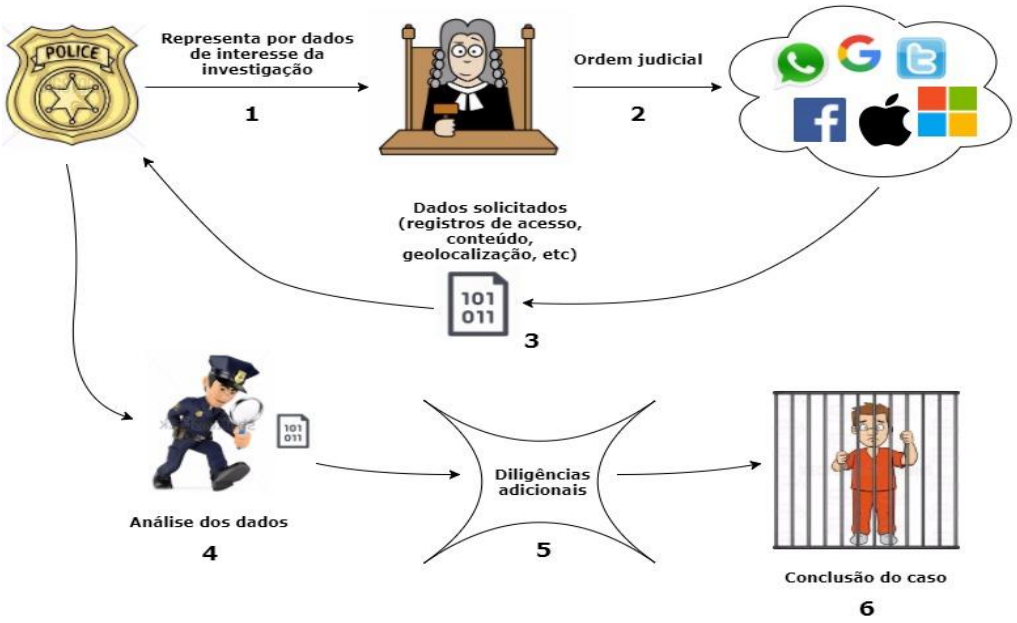
As etapas indicadas acima são, em regra, as adotadas na investigação da grande maioria dos casos delituosos que são levados ao conhecimento dos órgãos estatais de investigação, pois não há como ser diferente, uma vez que a descoberta da autoria de um crime no qual o autor utiliza o pseudoanonimato depende, na grande maioria das vezes, de dados que não estão disponíveis abertamente na rede mundial e são detidos e protegidos pelas empresas provedoras de aplicações de Internet e de conexão.

Conforme lecionam Wendt e Jorge (2013), os passos acima expostos são inter-relacionados um ao outro, sendo que a etapa destacada se encontra no caminho crítico do procedimento de investigação, pois é justamente a que é utilizada para obtenção dos dados cruciais para a elucidação do crime, sejam eles dados cadastrais, registros de acesso à aplicação, registros de conexão ou mesmo o conteúdo propriamente dito.

Sem o fornecimento desses dados pelas empresas, e esgotadas as buscas por informações em fontes abertas, a investigação pode estar fadada ao insucesso, pois se detém justamente na fase mais sensível para a obtenção de dados de autoria e/ou materialidade, devido a uma eventual negação de fornecimento dos dados solicitados.

De forma simplista, essa etapa da investigação até a conclusão do caso obedece ao seguinte fluxo:

Figura 6: Fluxo de ações da investigação de crimes cibernéticos



Fonte: Autor.

Deve-se mencionar que os dados solicitados não se referem somente a dados estáticos, pretéritos, mas também a dados de interceptação telemática, em tempo real. Peron (2012, p. 7) elenca que a interceptação telemática é "a ciência que lida com captura, registro e análise de tráfego de rede interceptado para detecção de intrusões e sua investigação".

Por conseguinte, se a autoridade policial não obtiver os dados solicitados mediante a via judicial dos provedores de aplicações, em muitos casos, não se conseguirá prosperar na investigação e, logo, não se alcançará a autoria do delito.

5 Dispositivos legais

A Lei Federal nº 12.965, de 23 de abril de 2014, conhecida como Marco Civil da Internet, não é um diploma legal que trate especificamente de matéria penal ou processual penal, pois o seu cerne é de fundo civil. Na redação de seu artigo 1º, tem-se:

> Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria (BRASIL, 2014).

Seus artigos 2º e 3º apontam para fundamentos e princípios que disciplinam o uso da Internet no Brasil, *in verbis*:

> Art. 2º A disciplina do uso da Internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:
> I - o reconhecimento da escala mundial da rede;
> II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;
> III - a pluralidade e a diversidade;
> IV - a abertura e a colaboração;
> V - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VI - a finalidade social da rede.
>
> Art. 3º A disciplina do uso da Internet no Brasil tem os seguintes princípios:
> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei;
> IV - preservação e garantia da neutralidade de rede;
> V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
> VII - preservação da natureza participativa da rede;
> VIII - liberdade dos modelos de negócios promovidos na Internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.
> Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte (BRASIL, 2014).

Oliveira (2014, p. 5) bem aponta que o Marco Civil da Internet não é uma "normativa deserta, isolada das demais fontes jurídicas", é um foco de irradiação normativa que pauta o comportamento dos indivíduos no mundo virtual.

Não é uma lei, portanto, focada na matéria de cibercrimes, entretanto tem reflexos diretos na investigação criminal dessa natureza de delitos no Brasil, principalmente devido à Seção II – "Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas", dentro do Capítulo III – "Da provisão de conexão e de aplicações de Internet", a qual dispõe, em seus artigos de 10 a 17, de instrumentos que disciplinam justamente a guarda de informações pelas empresas provedoras de aplicações de Internet e de conexão e o fornecimento dessas informações às autoridades.

Oliveira (2014, p. 12) continua seu trabalho elucidando que o artigo 11 do Marco Civil da Internet disciplina que empresa estrangeira, mesmo que não possua filial no Brasil, mas que oferte serviço ao público brasileiro, deverá obrigatoriamente respeitar a legislação brasileira. É o que se vê na letra da lei, em especial no parágrafo 2º do referido dispositivo:

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de Internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

> § 1º O disposto no **caput** aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.
>
> § 2º O disposto no **caput** aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil (BRASIL, 2014).

Em consonância com o artigo 11, o artigo 10 do Marco Civil da Internet e seus parágrafos são, para o tema analisado no presente trabalho, bastante relevantes, pois dispõem o seguinte:

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de Internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
>
> § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no **caput**, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.
>
> § 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º.
>
> § 3º O disposto no **caput** 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.

Na análise dos dispositivos supra, fica claro que a referida lei quis dar caráter de sigilo aos registros de conexão e de acesso, somente dando acesso a esses dados às autoridades mediante ordem judicial, sendo que Soares e Zanin (2015, p. 25), em se tratando do fornecimento de endereço IP, muito acertadamente, pontuam:

> [...] seja pela proteção do direito individual em detrimento ao direito coletivo, seja pelo interesse econômico do mercado da Internet, restou pela lei estabelecida, a burocratização para obtenção de um dado cadastral (endereço IP) que somente tem utilidade em auxiliar a identificação de dados maiores, como qualificação e endereço físico do usuário, que a mesma lei dispensa a autorização judicial.

É mister destacar, no entendimento dos autores, que a burocratização de acesso a um dado cadastral pelas autoridades policiais leva à morosidade na investigação, pois aumenta o tempo de espera por um dado que, muitas vezes, se mostra como essencial na apuração do crime.

Outro dispositivo legal que se deve mencionar é a Lei nº 9.296, de 24 de julho de 1996, conhecida como Lei de Interceptação Telefônica (LIT). Em meados da década de 1990, a Internet no Brasil já era utilizada, mas ainda não tão difundida.

Apresentam-se o artigo 1º da Lei e seu parágrafo 1º, *in verbis:*

> Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça.
>
> Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática (BRASIL, 1996).

Verifica-se que, em um diploma que possui mais de vinte anos, já havia previsão legal para interceptações de fluxo de comunicações em sistemas de informática e telemática[21], que nada mais fez que regulamentar o texto encontrado no artigo 5º, inciso XII, da Constituição da República Federativa do Brasil:

> 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; (BRASIL, 1988).

Nessa senda, Gomes e Maciel (2014) afirmam que a lei tem incidência nas comunicações telemáticas, inclusive nas atividades dessa natureza realizadas por telefones. Para os doutrinadores, não admitir que a comunicação telemática por telefone esteja sujeita à interceptação significa "retirar dos órgãos da persecução penal um instrumento valioso, principalmente nos dias atuais, de investigação e apuração da verdade real". Sabiamente, os autores discorrem que o crime organizado não opera sem o uso da informática, e rechaçar a aplicação da lei de interceptações telefônicas nessa modalidade de comunicação é deixar o criminoso da era digital fora do alcance do Estado.

Ademais, Baracho, Argolo e Diniz (2017, p. 11) bem recordam que o STF já se manifestou sobre eventual discussão de que o parágrafo único do artigo 1º da LIT seria inconstitucional, devido à interpretação gramatical do inciso XII do artigo 5º da CR, que somente autorizaria a interceptação de comunicações telefônicas, negando medida liminar em sede de Ação Direta de Inconstituconalidade (ADIn nº 1.488-9/DF).

[21] Comunicação que resulta do uso combinado de qualquer forma de telecomunicação com informática, conforme Gomes e Maciel (2014, p. 82).

No mesmo diapasão, da possibilidade de aplicação da Lei de Interceptação Telefônica ao tema em foco neste trabalho, Starr (2017, p. 97) faz uma interessante correlação da referida lei com o artigo 10, parágrafo 2º, do Marco Civil da Internet, o qual não se pode melhor elucidar que a citação *ipsis verbis*:

> No tocante ao pedido de interpretação conforme a Constituição, no art. 10, § 2º, da Lei n. 12.965/2014, de modo a limitar o seu alcance aos casos de persecução criminal, entendemos ser evidente que, uma vez que a disponibilização do conteúdo deve ocorrer "na forma que a lei estabelecer", impõe-se a aplicação da Lei n.º 9.296/1996, seja pela previsão contida no art. 1º, caput, deste último diploma legal, que faz referência à interceptação de comunicações telefônicas, de qualquer natureza, seja em decorrência do parágrafo único, ao dispor que a legislação em comento aplica-se às comunicações em sistema de informática ou telemática.

Dois anos mais recente que a Lei de Interceptações Telefônicas, a Lei Federal nº 9.613, de 3 de março de 1998, conhecida como a Lei de Lavagem de Dinheiro, recebeu modificações substanciais através da Lei nº 12.683, de 2012, que inclui, entre outros, o seguinte artigo:

> Art. 17-B. A autoridade policial e o Ministério Público terão acesso, exclusivamente, aos dados cadastrais do investigado que informam qualificação pessoal, filiação e endereço, independentemente de autorização judicial, mantidos pela Justiça Eleitoral, pelas empresas telefônicas, pelas instituições financeiras, pelos provedores de Internet e pelas administradoras de cartão de crédito.

Cavalcante (2012) aponta que, antes da modificação trazida pela Lei de 2012, era necessário que o delegado de polícia ou o membro do Ministério Público representasse judicialmente pelas informações pretendidas. Após a inclusão do artigo 17-B, não há mais necessidade da intervenção do Poder Judiciário na solicitação, tendo os sujeitos em tela acesso aos dados cadastrais do investigado, conforme se depreende da redação do artigo. Cavalcante, acertadamente, menciona que tais dados não são resguardados pelo sigilo de comunicações telefônicas, previsto constitucionalmente. Nesse sentido, o autor aponta seguintes precedentes do STJ:

> (...) Não estão abarcados pelo sigilo fiscal ou bancário os dados cadastrais (endereço, nº telefônico e qualificação dos investigados) obtidos junto ao banco de dados do Serpro. Embargos parcialmente acolhidos, com efeitos infringentes, para dar parcial provimento ao recurso.
> (EDcl no RMS 25.375/PA, Rel. Min. Felix Fischer, Quinta Turma, julgado em 18/11/2008, DJe 02/02/2009)
>
> (...) frise-se que o inciso XII do artigo 5º da Constituição Federal assegura o sigilo das comunicações telefônicas, nas quais, por óbvio, não se inserem os dados cadastrais do titular de linha de telefone celular.

> (HC 131.836/RJ, Rel. Min. Jorge Mussi, Quinta Turma, julgado em 04/11/2010, DJe 06/04/2011)

O mesmo autor vai mais longe: entende que a previsão trazida pelo artigo 17-B pode ser estendida para investigações de outros crimes, não apenas a lavagem de dinheiro, não havendo qualquer sentido na proibição da aplicação do dispositivo a outros delitos.

Dispositivo bastante semelhante ao elencado pela Lei de Lavagem de Dinheiro é trazido na nova Lei de Combate ao Crime Organizado, a Lei Federal nº 12.850, de 2 de agosto de 2013, que revogou a Lei nº 9.034, de 3 de maio de 1995. O artigo 15 da Lei nº 12.850 de 2013 traz a seguinte redação:

> 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 pela Justiça Eleitoral, empresas telefônicas, instituições financeiras, provedores de Internet e administradoras de cartão de crédito.

É inegável a comparação com o artigo 17-B da Lei nº 12.683, de 2012, cristalizando a intenção do legislador em desnudar de sigilo os dados cadastrais no âmbito da investigação criminal.

Sannini Neto (2013) aponta que a recusa no fornecimento dos dados cadastrais constitui crime tipificado pelo artigo 21 da Lei de Combate ao Crime Organizado, sendo punido com reclusão de 6 meses a 2 anos e multa. O mesmo autor enfatiza que o poder requisitório do delegado de polícia se atina aos dados cadastrais do investigado, conforme a letra da lei. Demais dados referentes ao sigilo bancário ou conteúdo de comunicações telefônicas continuam sujeitos à cláusula de reserva jurisdicional.

6 Resistência oferecida por alguns provedores de aplicação de internet

Durante a investigação policial de um crime que ocorreu na Internet, ou que a utilizou como meio, dados detidos pelas empresas provedoras de aplicação de Internet ou de conexão são, na grande maioria das vezes, cruciais para a elucidação da autoria e materialidade do delito.

Em investigações desencadeadas pelo Núcleo de Combate aos Cibercrimes – NUCIBER da Polícia Civil do Paraná – unidade especializada na prevenção e repreensão de crimes cibernéticos, com atribuição em todo o estado do Paraná, criada através da Resolução nº 293/05 SESP-PR, em 18 de novembro de 2005 – a práxis demonstra que a obtenção dos registros de conexão juntos aos provedores de conexão brasileiros não são o principal

problema enfrentando pelas autoridades. Na maioria dos casos, as empresas são sediadas em território brasileiro, possuem infraestrutura administrativa, jurídica e de tecnologia domésticas e fornecem, mediante requisição via ofício da autoridade policial ou MP, os dados pretendidos para comporem a investigação. Em caso de não atendimento da solicitação extrajudicial, ainda há possibilidade de a autoridade policial representar ou o MP requerer judicialmente os dados, sendo que diante de ordem emanada por juiz, resta às empresas provedoras de conexão atender à decisão judicial, sob pena de incorrerem em crime de desobediência.

Entretanto, no fluxo da investigação, antes da etapa supramencionada, é necessário obter o registro de acesso ou mesmo o conteúdo – sejam pretéritos, sejam em tempo real (interceptação telemática) – junto ao provedor de aplicação de Internet. É nessa etapa que as autoridades brasileiras envolvidas na investigação criminal vêm enfrentando problemas. Scherkerkewitz (2014, p. 108) salienta que tal situação permeia um equilíbrio delicado entre direito à intimidade e privacidade e o direito do Estado a investigar e punir crimes ocorridos por meio da Internet. Ainda complementa o autor que tal acesso a esses dados deve ser a exceção e não a regra. Nessa senda, verificou-se, através da análise de dispositivos legais, que arcabouço normativo para o acesso a esses dados, em casos de investigação criminal, não falta no ordenamento jurídico brasileiro.

Conforme bem apontam Soares e Zanin (2015, p. 25), antes da vigência do Marco Civil da Internet, o endereço IP era tratado pela jurisprudência como um dado cadastral, não revestido, portanto do sigilo constitucional. Entretanto, com a vigência do Marco Civil da Internet, houve a clara separação na lei entre dado cadastral e registros de conexão (IPs atrelados com data, hora e fuso horário):

> Apesar de o Marco Civil ter ratificado o entendimento jurisprudencial de que tanto a Polícia, quanto o Ministério Público têm o poder de requisitar dados cadastrais, sem a necessidade de autorização judicial, a lei dispôs expressamente acerca do sigilo que deve ser observado pelos provedores em relação aos registros de conexão e de acesso a aplicações de Internet. Assim, a lei foi de encontro à legislação especial penal e a jurisprudência dominante que também consideravam dispensável a autorização judicial para obtenção do endereço IP, que era incluído no rol de dados cadastrais, contudo, o Marco Civil terminou por separar este dado do rol de dados cadastrais passíveis de dispensa de autorização judicial.
> [...]
> O assoberbamento de feitos submetidos ao crivo do judiciário faz com que as decisões judiciais sejam lentas, e muitas vezes, ineficazes. O status atribuído ao endereço IP pelo Marco Civil transformou um dado meio em mais importante que o dado fim buscado através dele e, pela imposição de busca de autorização judicial, implicou o retardamento da investigação e, consequentemente, da identificação e punição do criminoso (SOARES; ZANIN, 2015, p. 27).

O que se vivencia, na prática, é exatamente o apontado pelos autores: uma dilatação temporal considerável nas investigações de crimes cibernéticos após a entrada em vigência do Marco Civil da Internet, quando dependem da obtenção de registros de acesso. Entretanto, apesar de que esse dispositivo legal em especial tenha tornado a investigação mais morosa, pois antes os registros eram fornecidos mediante requerimento extrajudicial das autoridades, ainda há a possibilidade de se obter o endereço IP através de ordem judicial.

O grande problema reside quando há necessidade de se obter informações mais específicas que os registros de acesso (IP) junto aos provedores de aplicação – algumas grandes empresas detentoras de redes sociais, serviços de e-mail, mensageiros instantâneos – que não atendem às ordens judiciais para fornecimento de dados como conteúdo de mensagens, geolocalização e interceptação em tempo real. Alegam impossibilidade técnica ou necessidade de Acordos de Assistência Judiciária em Matéria Penal (*Mutual Legal Agreement Treaties* – MLATs). Entretanto, o Superior Tribunal de Justiça já se manifestou contra essa alegação:

> RECURSO ORDINÁRIO EM MANDADO DE SEGURANÇA. INQUÉRITO POLICIAL. QUEBRA DE SIGILO TELEMÁTICO. CUMPRIMENTO INCOMPLETO DE ORDEM JUDICIAL. APLICAÇÃO DE MULTA DIÁRIA À EMPRESA RESPONSÁVEL PELO FORNECIMENTO DE DADOS (FACEBOOK). POSSIBILIDADE. VALOR DAS ASTREINTES. RAZOABILIDADE E PROPORCIONALIDADE.
>
> 1. Situação em que a FACEBOOK SERVIÇOS ONLINE DO BRASIL LTDA. impugna decisão judicial que, em sede de inquérito, autorizou a interceptação do fluxo de dados telemáticos de contas Facebook de investigados, sob pena de multa diária de R$ 50.000,00 (cinquenta mil reais).
> 2. Não há ilegalidade ou abuso de poder a ser corrigido, pois fica claro o cumprimento incompleto da decisão judicial que determinara o fornecimento de dados de contas perfis no Facebook de investigados, já que não foram trazidas todas as conversas realizadas no período de 13/10/2015 a 13/11/2015, tampouco as senhas de acesso, o conteúdo completo da caixa de mensagens, o conteúdo da linha do tempo (timeline) e grupos de que participam, além das fotos carregadas no perfil com respectivos metadados. **3. A mera alegação de que o braço da empresa situado no Brasil se dedica apenas à prestação de serviços relacionados à locação de espaços publicitários, veiculação de publicidade e suporte de vendas não exime a organização de prestar as informações solicitadas, tanto mais quando se sabe que não raras vezes multinacionais dedicadas à exploração de serviços prestados via Internet se valem da escolha do local de sua sede e/ou da central de suas operações com o objetivo específico de burlar carga tributária e ordens judiciais tendentes a regular o conteúdo das matérias por elas veiculadas ou o sigilo de informações de seus usuários.**
> **4. Por estar instituída e em atuação no País, a pessoa jurídica multinacional submete-se, necessariamente, às leis brasileiras, motivo pelo qual se afigura desnecessária a cooperação internacional para a obtenção dos dados requisitados pelo juízo.**
> ...
> 10. Recurso ordinário em mandado de segurança a que se nega provimento.

> (STJ - RMS: 55109 PR 2017/0215256-6, Relator: Ministro REYNALDO SOARES DA FONSECA, Data de Julgamento: 07/11/2017, T5 - QUINTA TURMA, Data de Publicação: DJe 17/11/2017. Grifos nossos.)

A fim de exemplificar tais situações na prática, procedeu-se a entrevista com o delegado-chefe do Núcleo de Combate aos Cibercrimes – NUCIBER da Polícia Civil do Paraná, doutor Demétrius Gonzaga de Oliveira, que está à frente dessa unidade desde o ano de 2006, a fim de que a autoridade policial relatasse e exemplificasse algumas respostas fornecidas por provedores de aplicações durante procedimentos de investigações policiais, nos quais houve alguma resistência no fornecimento de dados solicitados. Por motivos de sigilo, foram citados somente trechos das decisões judiciais e respostas dos provedores, bem como os dados sensíveis de ambos foram omitidos. Foram elencados dois casos.

6.1 Caso 1 – Nuciber - Google Brasil Internet Ltda

O caso analisado tratava-se de investigação de crime de estelionato, ocorrido através da Internet, no qual o autor, após ter sido devidamente identificado e ter sua prisão preventiva decretada em março de 2015, encontrava-se em local desconhecido, sendo considerado foragido da justiça. O NUCIBER, entre outras diligências, representou judicialmente a Google Brasil, com fulcro nos artigos 15, §3º e 22 da Lei 12.965/2014 e Lei 9.296/1996, por informações que auxiliassem a localizar o investigado, através de possível geolocalização de dispositivo Android em posse do mesmo. A seguir, segue-se trecho do ofício judicial que determinou à Google Brasil o fornecimento do desejado dado.

> Ilustríssimo Senhor
> DIRETOR NACIONAL EMPRESAS GOOGLE BRASIL INTERNET LTDA / ORKUT
>
> Senhor Diretor,
> Pelo presente, a fim de instruir os autos de Inquérito Policial nº xxxx, requisito a Vossa Senhoria, no prazo de 20 (vinte) dias, a remessa de relatório pormenorizado a este Juízo e ao Núcleo de Combate aos Crimes Cibertéticos – NUCIBER (através do e-mail xxxx) contendo:
>
> ...
>
> **3. Login e senha para acesso à plataforma Google que possibilite a localização geográfica EM TEMPO REAL de dispositivo móvel vinculado;**
>
> Todos referentes às seguintes contas:
> Conta Google *xxxxx@gmail.com*
> Conta Google *xxxxx@gmail.com*
>
> Tudo conforme solicitado pelo Núcleo de Crimes Cibernéticos nas investigações do Boletim de Ocorrência nº xxxxx.

> (Fonte: Núcleo de Combate aos Cibercrimes da Polícia Civil do Paraná. Grifos nossos.)

Diante da ordem judicial, a empresa Google a atendeu parcialmente, sendo que, no que diz respeito ao item 3, respondeu especificamente o seguinte:

> Excelentíssima Autoridade,
>
> Na qualidade de Custodiante de Dados a cargo de Google Inc., localizada em 1600 Amphitheatre Parkway, Mountain View, CA 94043, e constituída em Delaware, com sede na Califórnia, submeto esta carta.
> ...
> Por fim, no que diz respeito ao comando para interceptação do fluxo de dados, entende-se, salvo melhor juízo, que as disposições da Lei Federal nº 9.296/96 apenas se aplicam ao fluxo de comunicações em sistemas de informática e telemática (art. 1º, par. ún.), **razão pela qual a empresa está impossibilitada de realizar a interceptação de outros tipos de dados, tais como aquele listado no item "3" do ofício judicial**. Por esse motivo, pede-se, respeitosamente, seja reconsiderado o comando contido no item "3" do ofício judicial.
>
> (Fonte: Núcleo de Combate aos Cibercrimes da Polícia Civil do Paraná. Grifos nossos.)

Em face da resposta, restou ao NUCIBER trabalhar no caso apenas com dados pretéritos, não sendo fornecidos pela Google os dados em tempo real, através de "conta espelho" – método adotado por outros provedores de aplicações –, com a alegação de que a empresa está impossibilitada de realizar a interceptação de outros tipos de dados que não o fluxo de comunicações em sistemas de informática e telemática. Ora, tal requerimento da autoridade policial, deferida pelo poder judiciário, trata-se de fluxo de comunicações em sistemas de informática e telemática.

Por ter somente dados pretéritos para trabalhar, a localização do foragido dilatou-se por meses; foi necessário contar com o apoio de informantes e diligências em diversos endereços em Curitiba e em outras cidades do Paraná e Santa Catarina, até a localização do investigado na cidade catarinense de Canoinhas, em agosto de 2017, mais de dois anos depois da decretação da prisão.

6.2 Caso 2 – Nuciber - *Facebook*

O segundo caso analisado é um pedido de apoio da delegacia de polícia de cidade do interior do estado do Paraná ao NUCIBER. Trata-se de investigação de crime previsto no artigo 238 do Estatuto da Criança e Adolescente – ECA ("Prometer ou efetivar a entrega de filho ou pupilo a terceiro, mediante paga ou recompensa: Pena - reclusão de um a quatro anos,

e multa"). A denúncia que chegou às autoridades narra a negociação da entrega de um recém-nascido mediante pagamento, que ocorria através de mensagens privadas na rede social *Facebook* por meio dos perfis dos autores do delito.

Diante disso, a autoridade policial do NUCIBER representou judicialmente pelas seguintes informações junto ao *Facebook*:

> ...
> Diante do exposto, visando ainda a elucidar a origem e respectiva autoria do delito investigado, outra alternativa não resta senão requerer a Vossa Excelência:
> a) se digne em expedir OFÍCIO, dirigido à empresa FACEBOOK SERVIÇOS ONLINE DO BRASIL LTDA, cuja sede está localizada no endereço Av. Bernardino de Campos, 98, 4º andar – sala 28, bairro Paraíso, São Paulo-SP, CEP 04004-040 que em obediência a ordem judicial:
> i) a imediata QUEBRA DE SIGILO DE DADOS TELEMÁTICOS, devendo a empresa FACEBOOK informar, em caráter de urgência, a esse r. Juízo os dados cadastrais (e-mail, telefone), bem como seus respectivos log´s de acesso e IP´s de criação e administração (envio e recebimento de mensagens) dos internautas que utilizam as contas:
> https://www.facebook.com/xxxxxxxxxx
> https://www.facebook.com/yyyyyyyyyy
> ii) Cópia integral (mídia digital em formato PDF) de todas as conversas "In Box" ali contidas, desde a data de criação dos referidos perfis;
> iii) **A imediata INTERCEPTAÇÃO DE FLUXO DE DADOS TELEMÁTICOS das respectivas contas informadas acima nos termos do artigo 1º, parágrafo único, da Lei 9.296/96, pelo prazo de quinze dias, devendo o provedor de acesso das referidas contas criar uma "conta espelho", cujo dados (login e senha) devem ser enviados via e-mail ao NUCIBER (cibercrimes@pc.pr.gov.br) para monitoramento da conta**. O provedor deverá, ainda, ao final do prazo da interceptação, remeter cópia (em mídia e em papel) a esse r. Juízo de todas as mensagens recebidas e enviadas (e eventuais arquivos anexos). Por fim, deverá o provedor armazenar todas essas informações até a completa finalização das investigações.
> [...]
>
> (Fonte: Núcleo de Combate aos Cibercrimes da Polícia Civil do Paraná. Grifos nossos.)

O Juiz de Direito da vara criminal para a qual a demanda foi distribuída, diante da representação da autoridade policial e ouvido o Ministério Público, proferiu a seguinte decisão:

> ...
> DEFIRO, com fundamento no artigo 5º, inciso XII, da CR/88, o pedido de quebra de sigilo de dados telemáticos, bem como de interceptação de fluxo telemático, pelo prazo de 15 dias, das seguintes contas de rede social "FACEBOOK":
> https://www.facebook.com/xxxxxxxxxx
> https://www.facebook.com/yyyyyyyyyy
> Oficie-se à empresa FACEBOOK SERVIÇOS ONLINE DO BRASIL LTDA., a fim de que esta (i) informe os dados cadastrais dos proprietários das referidas contas (e-mail e telefone), seus logins de acesso e IPs de criação e administração (envio e recebimento de mensagens) (Prazo: 10 dias); (ii)

> encaminhe cópia integral, em formato PDF, de todas as conversas "in box" desde a data de criação dos mencionados perfis (Prazo: 10 dias); (iii) promova a interceptação de fluxo de dados telemáticos das supramencionadas contas, pelo prazo de 15 (quinze) dias, criando uma conta espelho, cujos dados deverão ser fornecidos à autoridade policial, via e-mail (cibercrimes@pc.pr.gov.br), para o monitoramento da conta (Prazo: imediatamente);...
>
> (Fonte: Núcleo de Combate aos Cibercrimes da Polícia Civil do Paraná.)

Submetida a ordem à empresa *Facebook* Serviços Online do Brasil Ltda, a mesma respondeu nos seguintes termos:

> Prezados Senhores,
> O seu pedido foi processado e os registros estão prontos para download a partir do nosso sistema de pedidos online. O número do pedido é xxxx.
> ...
> Nós divulgamos apenas informações básicas do usuário, em resposta ao seu pedido. **Mensagens, comentários, fotos e outros conteúdos só poderão ser divulgados através de um mandado de busca e apreensão obtido de acordo com 28 U.S.C. § 1782, ou em conformidade com o Acordo de Assistência Judiciária em Matéria Penal entre o Governo da República Federativa do Brasil e o Governo dos Estados Unidos da América (Decreto n. 3810/2001)**. Por favor, contacte a autoridade compentente do seu governo para mais informações.
> Nós ficamos felizes por continuar a cooperar com você.
>
> Atenciosamente,
> Law Enforcement Response Team
> [...]
> (Fonte: Núcleo de Combate aos Cibercrimes da Polícia Civil do Paraná. Grifos nossos.)

Verifica-se, portanto, que a empresa *Facebook* exige, para o fornecimento de diversos dados importantes à investigação criminal, a utilização de Acordos de Assistência Judiciária em Matéria Penal, o qual vai contra o julgado do STJ estudado neste trabalho.

Uma vez ciente da resposta negativa do *Facebook*, o Juiz de Direito determinou multa diária de R$ 100.000,00 (cem mil reais), limitada a R$ 2.000.000,00 (dois milhões de reais), bem como intimação pessoal do diretor da empresa para que cumpra a ordem judicial em 48 horas, sob pena de incorrer em crime de desobediência. Mesmo diante de tal constrição financeira e penal, a empresa ignorou a ordem emanada, continuando a justificar que os dados requisitados só podem ser fornecidos via Acordos de Assistência Judiciária em Matéria Penal.

Ao fim, não foi possível obter as provas que corroborariam para a investigação desencadeada pela delegacia de polícia que solicitou apoio ao NUCIBER.

Ambos os casos elencados acima representam exemplos práticos nos quais a autoridade policial representou judicialmente por dados necessários à investigação e o

magistrado deferiu os pedidos, porém os provedores de aplicações envolvidos não atenderam as demandas. Tais respostas negativas não só acarretaram o incremento do tempo das investigações, como também prejudicaram diretamente o trabalho da polícia judiciária na repressão aos crimes apurados.

6.3 Casos de repercussão nacional

Provavelmente os casos mais emblemáticos no Brasil de desobediência às ordens judiciais para o fornecimento de informações às autoridades durante uma investigação criminal foram os da empresa *WhatsApp*, que alegou não armazenar o conteúdo das mensagens nem ser possível interceptação, devido à criptografia ponta a ponta.

Starr (2017), com propriedade, critica fortemente a postura da empresa *WhatsApp* e de outras empresas de mensageiros instantâneos, crítica a qual se transcreve integralmente:

> Contudo, o que se nota pelo que afirmam autoridades de quase todos os territórios do mundo – inclusive Estados Unidos e União Europeia – é que aplicativos de mensagens vêm alegando o direito à privacidade e ao sigilo das comunicações como pilar inabalável. Essa atitude pode amparar a utilização para o cometimento de crimes graves, como tráfico de drogas, armas e de pessoas, divulgação de imagens e vídeos de pedofilia, sequestro, fraudes, homicídios, atentados terroristas e estupros. Desse modo, finge-se ignorar que não existe direito absoluto, bem como que a maioria dos usuários de tais aplicativos, na qualidade de não criminosos, não possuem interesse na proteção incondicional das mensagens trocadas com fins delituosos.
> [...]
> Importa ressaltar que a questão do afastamento do sigilo das comunicações voltadas ao crime já fora há muito superada e não há sentido em retomá-la cada vez que surgir novo recurso tecnológico destinado a facilitar a comunicação (STARR, 2017, p. 88-89).

A autora, nessas palavras e muito acertadamente, explanou a postura de tais empresas que, infelizmente, ignoram ordens judiciais e, até mesmo, a Carta Magna. Lamentavelmente, tal postura da empresa *WhatsApp* foi amplamente fortalecida pela comoção social, pela mídia, tribunais de segunda instância e até cortes superiores[22], os quais atacaram as decisões judiciais de primeira instância, que ordenaram o bloqueio do aplicativo após a negativa de fornecimento dos dados solicitados pela polícia.

A magistrada conclui seu texto com os seguintes trechos:

[22] "Bloqueio do WhatsApp viola direito à liberdade de expressão". Disponível em: https://epoca.globo.com/vida/experiencias-digitais/noticia/2016/07/lewandowski-cita-direito-liberdade-de-expressao-ao-suspender-bloqueio-do-whatsapp.html. Acesso em: 17 jun. 2018.

> No presente trabalho, após o estudo dos termos de uso do próprio aplicativo, ficou evidente a possibilidade de coleta de dados quando os administradores do aplicativo acreditam necessário. A página do aplicativo não especifica, contudo, quais os dados passíveis de coleta e compartilhamento.
>
> Os mesmos termos de uso preveem a possibilidade de não incidir a criptografia de ponta a ponta na hipótese de utilização de versão desatualizada do aplicativo. Não obstante, não se tem notícia de os descumprimentos judiciais virem acompanhados de efetiva comprovação de impossibilidade técnica de obtenção do conteúdo das mensagens (STARR, 2017, p. 106-107).

Nessa esteira, é possível que a atual política de privacidade da empresa *WhatsApp* seja a de não divulgar conteúdos de mensagens de usuários para autoridades, alegando que não há possibilidade técnica de realizar interceptações ou armazenamento em seu aplicativo. Entretanto, tecnicamente, bastaria à empresa desenvolver em sua infraestrutura de tecnologia e no código do aplicativo a possibilidade de desabilitar a criptografia e armazenar o conteúdo das mensagens de determinado usuário que seja "alvo" em uma investigação, obviamente diante de ordem judicial. Nesse sentido, Baracho, Argolo e Diniz (2017, p. 13) lecionam:

> Conforme já explanado, o WhatsApp utiliza um mecanismo de segurança que promete possibilitar o acesso do conteúdo das mensagens do aplicativo apenas aos usuários que se comunicam, por meio de chaves privadas que apenas estes acessam. Dessa forma, poderia se criar um argumento de que seria impossível a quebra do sigilo das comunicações dos dados. Porém, esse argumento não deve prosperar, haja vista a possibilidade de haver uma modificação do mecanismo de segurança do aplicativo para que seja possível conseguir as chaves privadas dos usuários, por determinação judicial e sob sigilo. Aliás, o que se deve enfatizar é a obrigação do WhatsApp realizar uma modificação do seu mecanismo de segurança para que esteja de acordo com o ordenamento jurídico.

Novamente, tais esquivos dessas empresas estão pautados mais em uma postura comercial que em uma impossibilidade técnica, quanto menos legal propriamente dita.

7 Considerações finais

Verificou-se que alguns provedores de aplicações de Internet são realmente reticentes em fornecer às autoridades policiais alguns dados de relevância durante uma investigação criminal, mesmo com ordem judicial.

Ao que parece, tais empresas adotam postura contestável, em que o direito à privacidade e ao sigilo se reveste de caráter absoluto. Não se pode esquecer que não há direito, mesmo fundamental, absoluto, se há de existir uma ponderação na vida prática, mormente em casos em que a lei assevera tal restrição. Mostrou-se que há amparo legal – e previsão constitucional – da possibilidade de, diante de ordem judicial, dados de atividades de

usuários de aplicativos e interceptações telemáticas serem realizadas em sede de inquérito policial. Alegações de impossibilidade técnica por parte das empresas em realizar tais fornecimentos de dados e/ou interceptações devido à inclusão de criptografia em seus produtos parecem um tanto quanto frágeis, pois tecnicamente bastaria desabilitar o referido recurso.

Em derradeira observação, é possível que tais negativas estejam mais pautadas em uma postura comercial das empresas – em não fornecer as informações requisitadas – do que propriamente uma impossibilidade técnica ou jurídica.

Referências

BARACHO, Daniel Duarte; ARGOLO JUNIOR, Cecílio; DINIZ, Liliane Amaral Janguiê Bezerra. A quebra do sigilo do WhatsApp como meio de prova aceito no direito pátrio: a necessidade de interceptação do sigilo das comunicações de dados para fins de persecução criminal. **Revista Jurídica Unigran,** Dourados, v. 19, n. 37, p.99-114, jun. 2017. Disponível em: http://www.unigran.br/revista_juridica/ed_anteriores/37/artigos/artigo06.pdf. Acesso em: 17 jun. 2018.

BARRETO JUNIOR, Irineu Francisco; LIMA, Marco Antonio. Marco Civil da Internet: Análise das decisões judiciais que suspenderam o aplicativo WhatsApp no Brasil – 2015-16. **Revista de Direito, Governança e Novas Tecnologias**, Curitiba, v. 2, n. 2, p. 37 – 52, jul/dez. 2016. Disponível em: http://indexlaw.org/index.php/revistadgnt/article/view/1484. Acesso em: 17 jun. 2018.

BECKER, Ana Maria Higuti. **Privacidade e liberdade de comunicação no ciberespaço**: limites à intervenção judicial brasileira no WhatsApp. 2016. 78 f. TCC (Graduação) - Curso de Direito, Setor de Ciências Jurídicas, Universidade Federal do Paraná, Curitiba, 2016. Disponível em: http://acervodigital.ufpr.br/handle/1884/46339. Acesso em: 17 jun. 2018.

BRASIL. Decreto-Lei nº 3.689, de 3 de outubro de 1941. **Código de Processo Penal**. Brasília, DF: Presidência da República, 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del3689Compilado.htm. Acesso em: 17 jun. 2018.

BRASIL. **[Constituição (1988)]**. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 17 jun. 2018.

BRASIL. **Lei nº 9.296, de 24 de julho de 1996**. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Brasília, DF: Presidência da República, 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L9296.htm. Acesso em: 17 jun. 2018.

BRASIL. **Lei nº 9.613, de 3 de março de 1998**. Dispõe sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores; a prevenção da utilização do sistema financeiro para os ilícitos previstos nesta Lei; cria o Conselho de Controle de Atividades Financeiras - COAF, e

dá outras providências. Brasília, DF: Presidência da República, 1998. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L9613.htm. Acesso em: 17 jun. 2018.

BRASIL. **Lei nº 12.683, de 9 de julho de 2012**. Altera a Lei nº 9.613, de 3 de março de 1998, para tornar mais eficiente a persecução penal dos crimes de lavagem de dinheiro. Brasília, DF: Presidência da República, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12683.htm#:~:text=LEI%20N%C2%BA%2012.683%2C%20DE%209,Art. Acesso em: 17 jun. 2018.

BRASIL. **Lei nº 12.850, de 2 de agosto de 2013**. Define organização criminosa e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a Lei no 9.034, de 3 de maio de 1995; e dá outras providências. Brasília, DF: Presidência da República, 2013. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em: 17 jun. 2018.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 17 jun. 2018.

BRASIL. Superior Tribunal de Justiça. **Recurso em Mandado de Segurança nº 55.109-PR**. Recorrente: F.S. O. do B.L. Recorrido: Ministério Público Federal. Relator: Ministro Reynaldo Soares da Fonseca, 07 de novembro de 2017. Disponível em: https://ww2.stj.jus.br/processo/revista/inteiroteor/?num_registro=201702152566&dt_publicacao=17/11/2017. Acesso em: 17 jun. 2018.

CAVALCANTE, Márcio André Lopes**.** Comentários à Lei n.° 12.683/2012, que alterou a Lei de Lavagem de Dinheiro. **Dizer o Direito**. *[S. l.*], 16 jul. 2012. Disponível em: http://www.dizerodireito.com.br/2012/07/comentarios-lei-n-126832012-que-alterou.html. Acesso em: 17 jun. 2018.

CERQUEIRA, Silvio Castro; ROCHA, Claudionor. Crimes cibernéticos: desafios da investigação. **Cadernos Aslegis**, Brasília, n. 49, p. 131-136, maio/ago. 2013. Disponível em: http://bd.camara.gov.br/bd/handle/bdcamara/27420. Acesso em: 17 jun. 2018.

DOMINGOS, Fernanda Teixeira Souza Domingos; RÖDER, Priscila Costa Schreiner. Obtenção de provas digitais e jurisdição na Internet. *In*: BRASIL. EMAG. Investigação e prova nos crimes cibernéticos. **Cadernos de Estudos**, São Paulo, v. 1, p. 55-84, 2017. Disponível em: http://www.trf3.jus.br/documentos/emag/Midias_e_publicacoes/Cadernos_de_Estudos_Crimes_Ciberneticos/Cadernos_de_Estudos_n_1_Crimes_Ciberneticos.pdf. Acesso em: 17 jun. 2018.

ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Márcio Pereira. **Desvendando a computação forense**. São Paulo: Novatec, 2011. 200 p.

GOMES, Luiz Flávio; MACIEL, Silvio. **Interceptação telefônica**: comentários à Lei 9.296, de 24.07.1996. 3. ed. rev e atual. São Paulo: Editora Revistas dos Tribunais, 2014. 224. p.

OLIVEIRA, Carlos Eduardo Elias de. **Aspectos principais da Lei nº 12.965, de 2014, o Marco Civil da Internet:** subsídios à comunidade jurídica. Brasília: Núcleo de Estudos e Pesquisas/CONLEG/ Senado, abr. 2014 (Texto para Discussão nº 148). Disponível em: https://www12.senado.leg.br/publicacoes/estudos-legislativos/tipos-de-estudos/textos-para-discussao/td-148-aspectos-principais-da-lei-no-12.965-de-2014-o-marco-civil-da-Internet-subsidios-a-comunidade-juridica. Acesso em: 17 jun. 2018.

OLIVEIRA, Marcos Aurélio Guedes de *et al*. **Guia de defesa cibernética na América do Sul.** Recife: UFPE, 2017. 162 p.

PERON, André. **SIT e CLIT**: ferramentas e metodologia para aprimoramento de investigações criminais utilizando interceptações de conexão à Internet. 2012. 132 f. Dissertação (Mestrado em Engenharia Elétrica) - Universidade de Brasília, Brasília, 2012. Disponível em: http://repositorio.unb.br/handle/10482/10471. Acesso em: 17 jun. 2018.

SANNINI NETO, Francisco. Nova lei das organizações criminosas e a polícia judiciária. **Jusbrasil**, [*s. l.*], 2013. Disponível em: https://franciscosannini.jusbrasil.com.br/artigos/121943694/nova-lei-das-organizacoes-criminosas-e-a-policia-judiciaria. Acesso em: 17 jun. 2018.

SCHERKERKEWITZ, Iso Chaitz. **Direito e Internet.** São Paulo: Editora Revista dos Tribunais, 2014. 171 p.

SCUDERE, Leonardo. **Risco digital na web 3.0.** Rio de Janeiro: Elsevier, 2015. 154 p.

SOARES, Valeska Maria Capelasso; ZANIN, Fabrício Carlos. Marco civil da Internet (lei 12.965/2014): a interpretação do endereço IP e suas implicações no ordenamento jurídico penal brasileiro. **Jus Societas,** Ji-paraná, v. 1, n. 13, p. 21-30, jan./jun. 2015. Disponível em: http://www.periodicos.ulbra.br/index.php/jsoc/article/view/2138. Acesso em: 17 jun. 2018.

STARR, Adriana Galvão. A dificuldade de acesso ao conteúdo das mensagens ilícitas trocadas via WhatsApp para uso em procedimento de investigação e ação penal. *In*: BRASIL. EMAG. Investigação e prova nos crimes cibernéticos. **Cadernos de Estudos**, São Paulo, v. 1, p. 85-109, 2017. Disponível em: http://www.trf3.jus.br/documentos/emag/Midias_e_publicacoes/Cadernos_de_Estudos_Crimes_Ciberneticos/Cadernos_de_Estudos_n_1_Crimes_Ciberneticos.pdf. Acesso em: 17 jun. 2018.

TEFFÉ, Chiara Antonia Spadaccini de. A responsabilidade civil do provedor de aplicações de Internet pelos danos decorrentes do conteúdo gerado por terceiros de acordo com o Marco Civil da Internet. **Revista Fórum de Direito Civil – RFDC**, Belo Horizonte, ano 4, n. 10, set./dez. 2015. Disponível em: http://www.editoraforum.com.br/wp-content/uploads/2015/12/A-responsabilidade-civil-do-provedor-de-aplicacoes-de-Internet.pdf. Acesso em: 17 jun. 2018.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos**: ameaças e procedimentos de investigação. 2. ed. Rio de Janeiro: Brasport, 2013. 369 p.