UNIVERSIDADE PRESBITARIANA MACKENZIE

Laís Guizelini Gibertoni

INTERCEPTAÇÃO TELEMÁTICA EM INVESTIGAÇÃO CRIMINAL E INSTRUÇÃO PROCESSUAL PENAL

São Paulo

2018

LAÍS GUIZELINI GIBERTONI

INTERCEPTAÇÃO TELEMÁTICA EM INVESTIGAÇÃO CRIMINAL E INSTRUÇÃO PROCESSUAL PENAL

Trabalho de Conclusão apresentado ao Curso de Graduação em Direito da Universidade Presbiteriana Mackenzie como requisito para obtenção do título de Bacharel.

ORIENTADOR: Prof. Ms. Ivan Luis Marques da Silva

São Paulo

2018

Gibertoni, Laís Guizelini

Interceptação telemática em investigação criminal e instrução processual penal, 48 f. il.; 30cm

Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade Presbiteriana Mackenzie, São Paulo, 2018.

Bibliografia: 46-48

1. Constituição Federal. 2. Marco Civil da Internet. 3. Criptografia. 4. Metodologia de Investigação de Crimes Cibernéticos.

LAÍS GUIZELINI GIBERTONI

INTERCEPTAÇÃO TELEMÁTICA EM INVESTIGAÇÃO CRIMINAL E INSTRUÇÃO PROCESSUAL PENAL

Trabalho de Conclusão apresentado ao Curso de Graduação em Direito da Universidade Presbiteriana Mackenzie como requisito para obtenção do título de Bacharel.

Aprovada em: ___/___/___.

BANCA EXAMINADORA

Prof. Ms. Ivan Luis Marques da Silva – Orientador
Universidade Presbiteriana Mackenzie

Prof. Examinador
Universidade Presbiteriana Mackenzie

Prof. Examinador
Universidade Presbiteriana Mackenzie

AGRADECIMENTOS

Cabe a mim, neste momento, expressar minha gratidão a diversas pessoas que contribuíram para a elaboração deste trabalho de conclusão de curso.

Primeiramente, a Deus, por conferir a possibilidade de concluir o presente curso, nesta instituição que tanto valorizo, por me dar sabedoria e força para lidar ante as adversidades ao longo desses anos, por ouvir meus medos e anseios e sempre me trazendo resposta de conforto e paz.

Aos meus pais, Antonio Gibertoni Junior e Iara Plepis Guizelini Gibertoni, por terem investido na minha formação acadêmica, sempre me incentivando, dando suporte e apoio nesta caminhada. Palavras não são capazes de exprimir como sou grata por estarem sempre ao meu lado, não permitindo que os percalços da vida me desanimassem.

Aos meus irmãos Henrique Guizelini Gibertoni e Gabriel Guizelini Gibertoni, que com muita alegria, fizeram com que esses cinco anos de curso passassem depressa de uma forma leve e descontraída.

Aos meus amigos, que estiveram ao meu lado, desde o primeiro dia de curso, tendo acompanhado passo a passo desta caminhada, ajudando tanto nas questões acadêmicas quanto nas pessoais. Aqueles que vivenciaram junto comigo os momentos de pressão e dificuldades, porém saíram vitoriosos e hoje, ainda juntos, podemos comemorar mais uma etapa da vida concluída.

Ao Professor Ivan Luiz Marques da Silva, orientador, pela humildade com que troca seu conhecimento, por me ensinar com paciência e bom humor, pelo auxílio e disposição.

Aos profissionais com quem trabalhei, por abrirem portas para mim, proporcionando oportunidades incríveis de aprendizado e crescimento profissional. Hoje são exemplos para mim de dedicação, honestidade e humildade.

Por fim, ao time de Voleibol Feminino Direito Mackenzie, que me proporcionou tamanhas alegrias e inúmeras vitórias, ensinando-me a ter disciplina, trabalhar em conjunto e manter a cabeça erguida em meio aos problemas, o qual eu tenho muito orgulho em ter feito parte.

"*Porque, onde está o teu tesouro, aí estará também o teu coração.*"

Mt. 6:21

RESUMO

Este trabalho versa sobre o instituto da quebra de sigilo de dados telemáticos e a interceptação de comunicações realizadas por intermédio da rede informatizada. Por meio de estudo de casos, da leitura bibliográfica aprofundada, bem como análise legislativa foi possível constatar que, em muitas situações, em decorrência da abertura legal proporcionada ao operador do direito, este meio de obtenção de provas acaba sendo utilizado de forma ordinária. A partir disso, chegou-se a conclusão que é necessário um aprimoramento da nossa legislação, bem como das técnicas judiciárias para o alcance desse tipo de provas, de modo para que sejam preservadas a intimidade, privacidade e confidencialidade das comunicações.

Palavras-chave: Interceptação. Comunicação. Dados cadastrais. Telemáticas.

ABSTRACT

This work deals with the institute of the breach of confidentiality of telematic data and the interception of communications carried out through the computerized network. Through a case study, in-depth bibliographic Reading, and legislative analysis, it was possible to verify that in many situations, due to the legal opening provided to the operator of the law, this apparatus to obtain evidence is used in a ordinary way. From this, it was concluded that it is necessary to improve our legislation, as well as judicial techniques to achieve this type of evidence, so as to preserve the intimacy, privacy and confidentiality of communications.

Keywords: Interception. Monitoring. Wiretapping. Communications. Register data. Telematics.

LISTA DE ABREVIATURAS

Art.	Artigo
CF.	Constituição
CP.	Código Penal
CPP.	Código de Processo Penal
HC.	Habeas Corpus
I.P.	Internet Protocol
MCI.	Marco Civil da Internet
STF.	Supremo Tribunal Federal
STJ.	Superior Tribunal de Justiça

SUMÁRIO

1- INTRODUÇÃO

O presente trabalho tem como escopo a análise sobre a possibilidade jurídica que o Estado tem de restringir o sigilo dos dados disponibilizados na rede, e em qual medida, bem como a possibilidade técnica em obter tais informações.

Na medida em que a tecnologia foi avançando, a sociedade passou a ter acesso a ferramentas virtuais que facilitam e agilizam muitas de suas tarefas, tanto cotidianas como profissionais.

A internet passou a ser um verdadeiro instrumento de interação, criação e transformação. Atualmente, pessoas físicas passam a representar usuários anônimos num ambiente virtual ilimitado e sem fronteiras.

O sistema de disponibilização de informação passa a ser cada vez mais complexo e articulado, para organização dos dados a fim de conferir acesso indiscriminado.

Com a inserção de mecanismos cada vez mais sofisticados, referentes a propagação da informação, houve certo estreitamento das relações no circuito privado, na medida em que confere possibilidade para interferências na intimidade da pessoa, mesmo em longas distâncias.

Em outras palavras, apesar de ser notório o estreitamento das relações, em decorrência dos avanços tecnológicos, ainda é possível o acesso a intimidade das pessoas, de qualquer lugar do mundo.

A internet pode ser caracterizada como um meio de comunicação que interliga milhares de pessoas, localizadas em qualquer lugar, proporcionando acesso a uma quantidade de informações inesgotáveis, praticamente, reduzindo-se então, cada vez mais, a distância tanto espacial quanto temporal.

Não obstante, a rede é dotada de características conflitantes, pois, ao mesmo tempo em que se está diante de um ambiente livre, sem limites geográficos, jurídicos e políticos, o usuário está submetido a uma supervisão, da qual ele não tem ciência, muito menos controle[1].

[1]Paesani e , L.M. 10/2014, ***Direito e Internet: Liberdade de Informação, Privacidade e Responsabilidade Civil, 7ª edição***, Atlas, São Paulo, SP, 2014, p. 21.

Assim, defronta-se perante um mundo no qual se tem a liberdade para agir da forma como lhe convir, porém está sujeito a certo monitoramento, onde cada passo dado será rastreado, e cada movimentação passa a ser registrada.

Por este motivo, importante se faz o envolvimento estatal neste campo, seja para regular o comportamento dos cidadãos no mundo virtual, seja para punir aqueles que se desviam das regras estipuladas, a fim de que se intervenha em casos de abusos, ou para prevenir comportamentos considerados como inadequados.

Para tanto, é necessário conferir ao Estado legitimidade para atuar desta forma, não podendo agir discricionariamente, devendo, então, submeter-se a regramentos jurídicos, de modo que saiba quando e como interferir na seara virtual.

Caso contrário, deparar-nos-íamos diante de "terras sem lei", onde não seriam encontradas normas que regessem as relações horizontais (entre particulares), muito menos normas de intervenção estatal (relação vertical), de modo a fazer com que o Estado se tornasse inimigo de seus próprios cidadãos.

Destarte, é possível verificar regras que permeiam entorno do tema em questão. Tais normas jurídicas configuram legitimidade ao Estado para invadir a privacidade no ambiente virtual, ou seja, é permitida ao Estado a violação à intimidade de outrem, desde que para atingir determinado propósito, como por exemplo, o monitoramento de conversas em tempo real, exclusão de conteúdo considerado ilícito, e dentre outras finalidades.

Dentro deste contexto, cumpre ressaltar que, não somente autoridades públicas têm interesse nos dados telemáticos de usuários da grande rede, muitas empresas de direito privado se utilizam de informações coletadas na internet com propósitos comerciais, por exemplo.

Atualmente, muitas dessas informações são utilizadas por empresas particulares, para traçar o perfil de consumidores a fim de direcionar anúncios de publicidade. Outro exemplo que pode ser citado é acerca da problemática na esfera trabalhista, no que tange ao acesso por parte do empregador de informações particulares de seus empregados, armazenadas no servidor da empresa, como forma de fiscalização.

Com isso, novos desenvolvimentos trazem consigo novas responsabilidades e riscos, razão pela qual se faz necessária uma regulamentação coesa e clara referente às relações no âmbito virtual.

Com efeito, a Internet tem o escopo de distribuir informações de forma ilimitada. Em contrapartida, as autoridades judiciárias estão sujeitas às normas e instituições do Estado e, portanto, a um território limitado. Sendo assim, possível se verificar o conflito e a dificuldade de aplicação dos controles judiciais na rede e a problematização de cumprimento das regras[2].

É cediço que há lacunas na legislação brasileira acerca deste tema e, em decorrência disso, abre-se margem para a criação de um espaço propício para práticas consideradas ilícitas, sejam estas evolvendo campos do direito civil e criminal, além atos de abusos de autoridades para intervir neste meio.

Nota-se, portanto, que o direito encontra dificuldades em se inserir neste universo, tendo em vista a existência de uma regulamentação escassa e fraca e um ambiente obscuro. Sendo assim, é clara a dificuldade que as autoridades judiciárias encontram em se impor em situações que envolvam a rede informatizada.

As mudanças impulsionadas pelas novas tecnologias, em especial pela evolução da internet, exigem, por sua vez, tanto uma adequação do direito a essa nova realidade como também normas jurídicas que subsidiem e acompanhem o desenvolvimento desta sociedade informatizada.

Por esta razão, e dentre outros motivos a serem expostos ao longo do presente trabalho, deparamo-nos diante da necessidade de regulação para que haja uma interferência, de forma legítima e discriminada, nas informações disponibilizadas na rede pelo particular.

Apesar da vigência das Leis ns. 12.735 de 2012, 12.737 de 2012 (conhecida como Lei Carolina Dieckmann), 12.965 de 2014 (doravante Marco Civil da Internet), e a mais atual Lei 13.709 de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD – sancionada pelo atual Presidente da República Michel Temer, em 14 de agosto de 2018), a intersecção entre o direito digital com o direito material e processual, mais especificadamente o processual penal, ainda possui falhas.

Além disso, para compreensão da matéria, não basta conhecimento jurídico, exige-se certa compreensão técnica sobre a rede informatizada e suas complexas interações.

---

[2]Paesani e , L.M. 10/2014, ***Direito e Internet: Liberdade de Informação, Privacidade e Responsabilidade Civil, 7ª edição***, Atlas, São Paulo, SP, 2014, p. 21.

Essencial se faz, portanto, para melhor aproveitamento dos meios que se tem a disposição, saber sobre o funcionamento da rede, como os dados são compartilhados, quem os armazena, onde são mantidos, as medidas a serem tomadas para obtenção de tais informações e como se utilizar destes para se alcançar seu almejado fim, qual seja, a produção probatória.

Hoje, o ambiente jurídico-digital passa por turbulências, pelo fato de o legislador brasileiro não dominar sobre o funcionamento da rede, bem como o aplicador do direito nesta área.

Por esta razão, a temática central deste trabalho se trata justamente na questão envolvendo os atos delituoso perpetrados no ambiente virtual e o envolvimento das autoridades para apuração dos fatos.

2- CONSTITUIÇÃO FEDERAL DE 1988 E A PRIVACIDADE DE DADOS

Atinentes ao assunto referente à proteção da privacidade do cidadão, ao longo do tempo, foram elaborados diversos estatutos e doutrinas[3].

Como célebre documento dogmático internacional, temos a Declaração Americana de Direitos e Deveres do Homem, de 1948, o qual conceitua o direito à privacidade como "*Artigo 5. Toda pessoa tem direito à proteção da lei contra os ataques abusivos à sua honra, à sua reputação e à sua vida particular e familiar.*"[4]

Outro diploma que merece destaque é a Declaração Universal dos Direitos do Homem, que reforça o preceito acima adotado: "*Ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques à sua honra e reputação. Toda pessoa tem direito à proteção da lei contra tais interferências ou ataques*" (art. 12)[5].

Consonante com os dispositivos expostos acima, o Pacto de São José da Costa Rica (Convenção Americana Sobre Direitos Humanos), ratificado pelo Brasil em 1992, assegura que "*2. Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação.*" de modo que "*3. Toda pessoa tem direito à proteção da lei contra tais ingerências ou tais ofensas*" (art. 11)[6].

Por sua vez, a Constituição Federal de 1988 estabeleceu em seu artigo 5, inciso XII, o direito a inviolabilidade da intimidade, aplicada à vida privada, de modo a garantir o sigilo das comunicações.

Este enunciado enfatiza a liberdade de expressão e de pensamento, desde que possa se identificar o indivíduo que se manifestou, bem como o direito à informação.

---

[3] LEITE Salomão, G. Lemos e R.(Coord.). 09/2014, **Marco Civil da Internet**, Atlas. Disponível em: Minha Biblioteca. p. 398.
[4] BRASIL. **Decreto no 678, de 1992 (promulgação)**: Convenção Americana sobre Direitos Humanos [anexo]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/D0678.htm. Acesso em: 02 de outubro de 2018;
[5] NAÇÕES UNIDAS. **Declaração Universal dos Direitos do Homem**. Disponível em: https://www.unicef.org/brazil/pt/resources_10133.htm Acesso em: 02 de outubro de 2018;
[6] BRASIL. **Decreto no 678, de 1992 (promulgação)**: Convenção Americana sobre Direitos Humanos [anexo]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/D0678.htm. Acesso em: 02 de outubro de 2018;

Em seu dispositivo, está delimitado[7]:

> 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.

Em consonância com este dispositivo, temos o inciso X, do mesmo artigo 5, da CF, o qual versa "*X- são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação*."

O direito a intimidade foi arduamente conquistado, de modo a ser garantido em nossa Lei Maior, tendo sido inserido no rol de direitos fundamentais, classificados como cláusulas pétreas.

Pode-se classificar privacidade como o direito de expor a intimidade de alguém, isto é, a liberdade de escolher o conteúdo que será tornado público, e aquele que permanecerá no íntimo do indivíduo[8].

Contudo, a regra da inviolabilidade das comunicações está acompanhada pela clausula de exceção, a qual delimita hipóteses de restrição a esse direito, especificadamente para fins de investigação criminal ou instrução processual penal.

Sendo assim, a quebra de sigilo telemática é, portanto, a exceção. Isto é, só pode ser aplicada de forma subsidiária, quando não houver outro meio tão capaz quanto a violação do sigilo, porém menos invasivo, de se atingir o resultado almejado, qual seja, identificar o indivíduo alvo da investigação, ou lastro probatório.

Atualmente o Poder Público detém legitimidade para a captação de informações de dados privados através de meios eletrônicos sofisticados, sob o fundamento de lhe caber a responsabilidade de segurança de seus cidadãos. Contudo, este poder conferido ao Estado de acesso a privacidade de seus cidadãos, pode acabar acarretando em um domínio estatal com consequências políticas e sociais graves.

---

[7]BRASIL, **Constituição Federal de 1988**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 03 de junho de 2018.

[8]RODRIGUEZ, Victor Gabriel. **Tutela penal da intimidade: perspectivas da atuação penal na sociedade da informação**. São Paulo: Atlas, 2008 xii, 261 p. ISBN 9788522450848;

Para tanto, foram estabelecidas certas formalidades legais que devem ser cumpridas, a fim de que a autoridade competente possa requisitar tais informações.

No entanto, hoje, a quebra de sigilo passou ser a regra, em muitas das vezes, sendo utilizada como primeira diligência investigatória, sem qualquer ponderação.

O Conselho Nacional de Justiça compatibilizou, no ano de 2017, que apenas em procedimentos criminais, foram determinados cerca de 27.032 (vinte e sete mil e trinta e dois) pedidos de quebra de sigilo (não há especificação sobre a natureza da quebra, podendo abranger as telefônicas, telemática, bancaria e financeira), como medidas cautelares[9].

Em muitas situações, a quebra de sigilo tem sido a primeira medida investigativa a ser tomada pela autoridade policial ao iniciar a apuração dos fatos. É possível verificar que os ditames estabelecidos em lei são deixados de lado por essas autoridades, os quais sobrepõe a necessidade de encontrar as provas para alcançar a suposta justiça, proteger vidas ou evitar que novos crimes aconteçam.

Temos como exemplo, a solicitação de quebra de sigilo formulada por autoridade policial no bojo de Boletim de Ocorrência. Primeiramente, cumpre esclarecer que o referido documento é um ato preparatório que ensejará um eventual inquérito policial. Caso o Delegado de Polícia entenda haver indícios de alguma prática delitiva, é decretada a instauração do inquérito com base no que fora colhido na lavratura do Boletim de Ocorrência.

Ocorre que, por ser um instrumento preparatório, podem ser tomadas algumas medidas investigativas, ausentes de quaisquer formalidades, para embasar eventual inquérito. Contudo, providências como requisição de quebra de sigilo, no caso do presente trabalho, a telemática, só pode ser feita quando de fato for essencial para a investigação, isto é, quando certamente já houver uma investigação oficial em andamento e, em paralelo, não for possível a obtenção das provas visadas por outros meios, e não para assegurar provável inquérito policial a ser instaurado preteritamente.

É fato que invadir a privacidade de outrem é o meio mais fácil e certeiro para obter a informação desejada, mas a legislação brasileira prevê ser o último subsídio para a garantia de provas, somente podendo ser feita quando não houver outra opção, justamente por ser a

[9] Disponível em: https://paineis.cnj.jus.br/QvAJAXZfc/opendoc.htm?document=qvw_1%2FPainelCNJ.qvw&host=QVS%40neodimio03&anonymous=true&sheet=shResumoDespFT; Acesso em 12 de julho de 2018.

alternativa mais invasiva e a que mais fere o direito a intimidade, tão valorizado pela nossa sociedade, e tão protegido pelo ordenamento jurídico nacional.

Enfim, o escopo da quebra de sigilo é a obtenção de provas para se chegar na pessoa em que se está investigando, ou o rastro deixado na internet. No entanto, há que se cumprir os requisitos legais para tanto. Caso não concorde com o regramento jurídico que delimita essa questão, há necessidade de alteração legislativa e não simplesmente criar manobras para se chegar no almejado fim.

Nesse sentido, conforme asseverado por Tércio Sampaio Ferraz Junior [10]:

> a publicidade dos atos processuais (visibilidade da coisa pública) é limitada pela intimidade: a lei pode exigir sigilo (art. 5o, LX), do mesmo modo que a publicidade das informações de interesse particular ou de interesse coletivo ou geral é limitada pelo sigilo necessário à segurança da sociedade e do Estado (art. 5o, XXXIII). Já por aí se observa que o direito à inviolabilidade do sigilo (faculdade) exige o sopesamento dos interesses do indivíduo, da sociedade e do Estado (objeto). Há casos em que a própria Constituição, como vimos, faz o sopesamento. Mas há outros em que o sopesamento aponta para outras relações possíveis nomeadamente, entre o direito ao sigilo e o dever de sigilo. Tudo isso mostra, em síntese, que, quando a Constituição garante a inviolabilidade do sigilo, o princípio do sopesamento exige que o interprete saiba distinguir entre o devassamento que fere o direito à privacidade, no seu objeto, em relação com outros objetos de outros direitos também protegidos pelo sigilo.

Ainda, no que tange a questão da proteção das correspondências conferida pela Constituição Federal de 1988, necessário se faz classificar a interceptação de comunicação e de dados do usuário[11].

Interceptar comunicações telemáticas envolve obter informações acerca do conteúdo das conversas travadas entre os usuários da rede, isto é, terceiro que invade a privacidade alheia para ter ciência do que se passa entre duas ou mais pessoas quando estão em seu íntimo, enquanto que a interceptação de dados telemáticos se trata do acesso aos registros codificados, referente ao meio como a comunicação fora realizada.

---

[10] FERRAZ JUNIOR, Tércio Sampaio. **Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado**. Cadernos de Direito Constitucional e Ciência Política, São Paulo, no 1, 1998, p. 79.

[11] GOMES, Luiz Flávio. **Interceptação telefônica: lei 9.296, de 24.07.1996**. São Paulo: Revista dos Tribunais, 1997. 278 p. ISBN 8520314996

Cumpre destacar sobre os conflitantes entendimentos sobre a exceção vigente no inciso XII, do supramencionado artigo 5. A maioria dos doutrinadores, entendem que esta restrição abarca tão somente o sigilo das comunicações, abrindo-se, então, a possibilidade de obtenção dos demais dados disponibilizados pelo usuário da rede, sem a necessidade de determinação judicial.

Isto porque, de acordo com este entendimento, o que se busca proteger é a intimidade dos cidadãos, a qual está intimamente ligada as comunicações, e não aos dados gerados ou fornecidos em decorrência do comportamento do usuário na internet.

Por outro lado, pode se concluir que esta exceção engloba tanto as comunicações entre os usuários quanto a transmissão de dados. Nesse sentido, Hugo Hoeschl reconhece que a chamada transmissão de dados é considerada uma forma de comunicação.

Com efeito, esse mesmo autor se utiliza do conceito de "dados" estabelecido no Decreto 97.057/1988, que altera a Lei de Regulamento Geral para a execução do Código de Telecomunicação (Lei no 4.117, de 1962) como sendo "*informação sistematizada, codificada eletronicamente, especialmente destinada a processamento por computador e demais máquinas de tratamento racional e automático da informação*" (art. 6o, item 23o).

Não obstante a isso, o item 158, deste mesmo artigo, classifica a transmissão de dados como "*forma de telecomunicação caracterizada pela especialização na transferência de dados de um ponto a outro*."

Sendo assim, passível a constatação de que a transmissão de dados é uma modalidade de comunicação de informações codificadas no âmbito virtual. Desta forma, resta claro a necessidade de ordem judicial para o fornecimento de dados telemáticos armazenados na rede, uma vez que também estão protegidos constitucionalmente.

O Marco Civil da internet traz consigo a possibilidade da interceptação de dados cadastrais independente de ordem judicial. Em decorrência disso, abriu-se a oportunidade para interpretações no sentido de que, em qualquer situação, é passível o fornecimento de dados cadastrais, sem determinação do judiciário, sob a alegação de que dados cadastrais nada mais são do que as informações pessoais que o próprio usuário disponibilizou ao provedor de aplicação ou conexão ao efetuar seu cadastro na rede. Assim, não estariam acobertados pela proteção constitucional da inviolabilidade, uma vez que o próprio cidadão os forneceu.

Contudo, conforme se infere do mencionado dispositivo com cautela, tendo em vista que, estes dados cadastrais apenas são fornecidos pelo indivíduo ao ingressar na internet, pois se vê obrigado, não lhe restando outra alternativa, senão apresentar as informações exigidas pelas operadoras de telefonia, ou serviços de aplicação, para poder ingressar no mundo virtual.

Ainda, no que tange a redação do inciso XII, do artigo 5, da Carta Magna, tem-se a inviolabilidade (i) das correspondências; (ii) das comunicações telegráficas; (iii) dos dados; e (iv) das comunicações telefônicas. Ora, não seria razoável a exceção limitar-se as comunicações telefônicas, telegráficas e de correspondências, deixando de lado apenas as de dados.

Nesse aspecto, o Egrégio Superior Tribunal de Justiça se posicionou no seguinte sentido:

> Como cediço, a Constituição Federal de 1988 prevê como garantias ao cidadão a inviolabilidade da intimidade, do sigilo de correspondência, dados e comunicações telefônicas, salvo ordem judicial.[12]

> Permanece vigente a Lei 12.965/2014, prevendo que o provedor responsável pela guarda dos registros de conexão e de acesso a aplicações de internet, bem como de dados pessoais e do conteúdo de comunicações privadas, será obrigado a disponibilizar as informações mencionadas mediante ordem judicial.[13]

Neste contexto, importa ressaltar o impasse da quebra de sigilo para outros fins, sem ser de investigação policial ou persecução penal. Atualmente, está sendo tema de debate no STF, em no bojo da ação direta de inconstitucionalidade n. 5527, no âmbito da qual discute-se, primordialmente, a inconstitucionalidade dos artigos 10,§2º e 12, incisos III e IV, ambos do Marco Civil da Internet[14].

---

[12] STJ. RHC 75.055/DF. Rel. Ministro Ribeiro Dantas, Quinta Turma. DJe 27/03/2017.
[13] STJ. RMS n.º 56.706/RS. Rel. Ministro Felix Fischer. Quinta Turma. DJe 09.05.2018.
[14] 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.
§ 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.
Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:
III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou
IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.

Proposta pelo Partido da República - PR - em 16 de maio de 2016, argumenta-se que os mencionados artigos violam a Constituição Federal, utilizando-se como paradigma os recentes julgamentos que acabaram por determinar a suspensão do aplicativo WhatsApp em todo território nacional, sob a alegada recusa da empresa em disponibilizar às autoridades judiciárias o conteúdo das mensagens trocadas pelos usuários que, naquele momento estavam sendo investigados criminalmente.

Dentre muitos argumentos trazidos para embasar a tese de inconstitucionalidade, sustenta-se que o mencionado §2, do artigo 10, ao permitir a disponibilização do conteúdo das mensagens privadas, desde que proferida ordem judicial para tanto, abre-se margem para a possibilidade de quebra de sigilo telemática fora das hipóteses elencadas na Constituição da República, quais sejam, a persecução penal, de modo a extrapolar os limites impostos constitucionalmente e, com isso, violando o princípio da inviolabilidade da privacidade

Esta ADI n. 5527 está pendente de julgamento, cuja relatoria é da Ministra Rosa Weber.

Resta evidente, portanto, a celeuma em torno da colisão entre os princípios constitucionais da liberdade de expressão e a privacidade da informação. Cumpre ressaltar que os princípios possuem a mesma carga valorativa no ordenamento jurídico, logo não há princípio superior ao outro[15].

Nesse sentido, havendo colisão entre eles deve ser aplicado o princípio da proporcionalidade, momento em que, levando-se em conta os fatos e os direitos do caso concreto em análise, realiza-se a ponderação entre eles, e consequentemente o sopesamento, para verificar adequadamente qual o princípio que deve prevalecer em determinada situação[16].

[15] MASSO, Fabiano Del; ABRUSIO, Juliana Canha; FLORÊNCIO FILHO, Marco Aurélio (Coord.). **Marco civil da internet:** lei 12.965/2014. São Paulo: Revista dos Tribunais, 2014. 268 p. ISBN 9788520353066. P. 31

[16] GOMES, Luiz Flávio. **Interceptação telefônica: lei 9.296, de 24.07.1996**. São Paulo: Revista dos Tribunais, 1997. 278 p. ISBN 8520314996

3- MARCO CIVIL DA INTERNET

Com o exponencial crescimento do mundo virtual nas últimas duas décadas, e sua presença cada vez mais marcante nas diversas áreas da vida cotidiana, com papel essencial nas relações pessoais, profissionais, comerciais e educacionais, acompanhado com o aumento do valor econômico associado ao meio digital, observou-se certo desvirtuamento do uso da rede e a disseminação de cometimentos de crimes neste ambiente.

Diante deste cenário, fez-se necessária a edição de normas para regular as relações decorrentes do mundo virtual, para assegurar segurança e legitimidade de suas ações.

Neste contexto, foi sancionada a Lei n 12.965, de 23 de abril de 2014, chamada de Marco Civil da Internet, que, embora seja uma lei aprovada às pressas, pode ser considerada como uma grande conquista para o Brasil, ante absorção da nova realidade vivida pelo arcabouço legal.

Elaborada com o objetivo de conferir maior segurança aos usuários, garantindo a privacidade e aplicação dos direitos humanos, acompanhado com o pleno exercício da cidadania no âmbito virtual, a mencionada Lei vem para, além disso, regulamentar questões envolvendo às explorações comerciais e a governança na rede.

O Marco Civil da Internet, foi a primeira lei elaborada de forma colaborativa envolvendo Governo, a sociedade brasileira, comunidade empresarial, especialistas técnicos e representantes acadêmicos, tendo sido estabelecidos princípios, garantias, direitos e deveres de usuários, provedores de serviços e demais agentes envolvidos com o uso da internet no Brasil.

O projeto de lei suscitou calorosos debates, uma vez que atingia diversos interesses, envolvendo os usuários da internet, provedores de conexão e aplicação, detentores de direitos autorais, autoridades regulatórias, judiciais e policiais.

Dentre os temas debatidos, vale ser mencionado (i) a neutralidade da rede (*net neutrality*), a qual se trata sobre a ausência de interferências dos fornecedores de acesso de banda larga na velocidade dos pacotes trafegados pela internet com o intuito de priorizar certos tipos de conteúdo em detrimento de outros; (ii) a guarda de registros de conexão e das aplicações de internet; (iii) responsabilidade dos provedores acerca de matérias ilegais divulgados em suas plataformas e (iv) armazenamento de dados no país, acompanhado do atendimento à legislação brasileira.

A internet é caracterizada por três elementos essenciais: (i) ser uma cadeia de redes interligadas entre si; (ii) existir em escala mundial; e (iii) ser um sistema de equipamentos que se comunicam por meio de uma mesma linguagem, de modo a permitir a circulação de informação através de conversações sequencias.

Pode-se dizer, portanto, que a mencionada Lei Federal, é constituída por três pilares, quais sejam: (i) a neutralidade da rede; (ii) liberdade de expressão; e (iii) privacidade.

No que tange à neutralidade da rede, delimita-se sobre o livre e indiscriminado tráfego de dados, de modo que não haja controle por nenhum ente público ou por empresas de direito privado sobre as informações que serão entregues aos usuários.

Quanto a liberdade de expressão, fundamento consolidado pela Constituição Federal, reforça a mesma liberdade de expressão, porém no ambiente virtual, na medida em que protege a intimidade, honra e a imagem dos usuários.

Por fim, com relação ao tema da privacidade de dados, parte-se da perspectiva de que as pessoas são detentoras de seus próprios dados, sendo assim dispõe sobre regras de consentimento para o tratamento de seus dados, exigindo transparência quanto a política de privacidade das empresas. Em decorrência disso, garante ao cidadão o poder de decidir sobre a exibição e uso de seus dados.

Assim, em seu artigo 2, foram estabelecidos os fundamentos do uso da internet no Brasil. Vale ressaltar, que dentre os fundamentos elencados neste artigo, merece destaque a liberdade de expressão, que, diferentemente dos demais, está estipulada no próprio caput, e não ao longo dos incisos. Com isso, pode-se verificar certa posição de destaque deste fundamento, com relação aos outros. Vejamos:

> 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.

Em seguida, o artigo 3 dispõe sobre os princípios norteadores do uso da internet:

> 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.

Nota-se que, em seus incisos II e III, há uma separação entre a proteção à privacidade e aos dados pessoais (na forma da lei), o que, mesmo estando intrinsicamente ligados um ao outro, evoca uma interpretação de que os dados pessoais possuem conceito distinto do da privacidade.

Por fim, temos o artigo 4, que versa sobre o escopo da utilização da grande rede mundial:

> Art. 4o A disciplina do uso da internet no Brasil tem por objetivo a promoção:
>
> I - do direito de acesso à internet a todos;
>
> II - do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos;
>
> III - da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; e
>
> IV - da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados.

Evidente que o legislador buscou tornar o acesso a internet mais democrático e generalizado, tendo em vista a importância ao exercício da cidadania a integração da sociedade no ambiente virtual.

Com isso, em consonância com os supramencionados dispositivos, tem-se o artigo 7, da mesma lei, inserido no capítulo II, o qual trata, por sua vez, sobre os direitos e garantias assegurados aos usuários da internet no Brasil, como pode se verificar:

> Art. 7o O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
>
> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
>
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
>
> IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;
>
> V - manutenção da qualidade contratada da conexão à internet;
>
> VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;
>
> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
>
> VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
>
> a) justifiquem sua coleta;
>
> b) não sejam vedadas pela legislação; e
>
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
>
> IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
>
> X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;
>
> XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;
>
> XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e
>
> XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.

Neste aspecto, os incisos II e III trazem à tona a questão anteriormente debatida sobre a abrangência da proteção constitucional alcançar apenas o conteúdo das comunicações,

excluindo os dados estáticos, como por exemplo os cadastrais e metadados [17]. Agora o referido dispositivo elucida que esta proteção se estende também aos referidos dados, não somente os que estão em trânsito, mas também os armazenados [18].

Importante destacar a ressalva trazida no artigo 10, o qual reitera a proteção dada aos registros de conexão e de acesso a aplicação da internet, bem como dos dados cadastrais e conteúdos de comunicações privadas.

Contudo, em seu parágrafo 2, permite a interceptação das comunicações particulares, desde que com ordem judicial. Por outro lado, o parágrafo 3 dispensa a ordem judicial, quando envolver a quebra de sigilo apenas quanto aos dados pessoais dos usuários, porém esclarece que apenas nas hipóteses em que a lei estabelecer. Vejamos:

> 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.**
>
> § 4o As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.

Sendo assim, para que seja desnecessária a ordem judicial para o fornecimento de dados cadastrais, é preciso que haja previsão legal comportando esta ressalva.

---

[17] "Os metadados são marcos ou pontos de referência que permitem circunscrever a informação sob todas as formas, pode se dizer resumos de informações sobre a forma ou conteúdo de uma fonte. * O prefixo "Meta" vem do grego e significa "além de". Assim Metadados são informações que acrescem aos dados e que têm como objectivo informar-nos sobre eles para tornar mais fácil a sua organização." Disponível em: https://www.metadados.pt/oquesaometadados. Acesso em 05 de outubro de 2018.

[18] MASSO, Fabiano Del; ABRUSIO, Juliana Canha; FLORÊNCIO FILHO, Marco Aurélio (Coord.). **Marco civil da internet: lei 12.965/2014**. São Paulo: Revista dos Tribunais, 2014. 268 p. ISBN 9788520353066. P. 146

Nesse sentido, diversos diplomas abarcam essa exceção, como por exemplo, na (i) Código de Processo Penal, em seu artigo 13-A[19]; (ii) Lei Federal nº 12.683/12 (Lei de Lavagem de Dinheiro), em seu artigo 17-B [20]; (iii) Lei Federal nº 12.850/13 (Lei de Organização Criminosa), no artigo 15 [21]; e (iv) a Lei Federal 13.260/16 (Lei Antiterrorismo), no artigo 16[22].

Contudo, em decorrência da redação do mencionado artigo 10, §3, muitas autoridades têm interpretado no sentido de desnecessidade de ordem judicial para o fornecimento de dados cadastrais [23] em qualquer situação, independente do crime a ser apurado.

Nos termos da previsão expressa contida no artigo 15, §3 (inserido na Subseção III, Da Guarda de Registros de Acesso de Aplicações de Internet e Provisão de Aplicação), o qual dispõe sobre a exigência de decisão judicial deferindo a quebra de sigilo em qualquer situação.

> Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.
>
> § 1o Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no caput a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado.
>
> § 2o A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no caput, observado o disposto nos §§ 3o e 4o do art. 13.
>
> § 3o **Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial**, conforme disposto na Seção IV deste Capítulo.
>
> § 4o Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual

[19] "Art. 13-A. Nos crimes previstos nos arts. 148 , 149 e 149-A , no § 3º do art. 158 e no art. 159 do Decreto-Lei no 2.848, de 7 de dezembro de 1940 (Código Penal) , e no art. 239 da Lei n º 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente) , o membro do Ministério Público ou o delegado de polícia poderá requisitar, de quaisquer órgãos do poder público ou de empresas da iniciativa privada, dados e informações cadastrais da vítima ou de suspeitos. (Incluído pela Lei nº 13.344, de 2016) (Vigência)."

[20] "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."

[21] "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."

[22] "Art. 16. Aplicam-se as disposições da Lei nº 12.850, de 2 agosto de 2013, para a investigação, processo e julgamento dos crimes previstos nesta Lei."

[23] Cumpre ressaltar que o Decreto n. 8.771/ de 2016 conceitua dados cadastrais como qualificação pessoal (nome, prenome, estado civil e profissão), endereço e filiação.

> vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

No que tange ao armazenamento e tratamento dos dados, deparamo-nos com a questão da territorialidade, uma vez que, em certos casos, apesar de o provedor ter sede localizada no Brasil, os dados coletados estão salvaguardados no estrangeiro, geralmente na matriz da empresa. Nesta situação, há necessidade de expedição de carta rogatória para a sede principal da empresa responsável pela manutenção dos dados? A lei exige estrutura técnica para o fornecimento de dados relacionados ao Brasil?

O Marco Civil da Internet traz esta questão, para evitar conflitos relacionados a territorialidade e o alcance da jurisdição brasileira no exterior.

Nesse sentido, temos o artigo 11, da referida Lei, no qual é expressa a aplicação da legislação brasileira sobre os dados pessoais e de comunicação quando tratados, coletados, armazenados ou guardados, em território brasileiro, por provedores, tanto de aplicação, quanto de conexão, conforme pode se verificar:

> 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.
>
> § 3o Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.
>
> § 4o Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

Ressalta-se que, o mencionado artigo traz os registros de dados pessoais dos usuários, bem como os de comunicação, não havendo segregação entre ambos, sendo os dois passíveis de aplicação da legislação nacional quando envolver dados coletados no Brasil. Necessário

salientar a exigência de que o terminal eletrônico precisa se encontrar localizado Brasil, para que esses dados estejam ao alcance da jurisdição brasileira.

Importa destacar, ainda tratando a respeito do artigo 11, sobre o seu parágrafo 2, o qual traz à tona a questão envolvendo pessoas jurídicas não sedeadas no Brasil. Conforme se pode inferir da leitura do mencionado dispositivo, resta evidente que basta haver representação da empresa em território brasileiro que a companhia estará sujeita ao regramento jurídico pátrio quanto ao tratamento de dados telemáticos e, caso a empresa não detenha estabelecimento no Brasil, porém uma das integrantes pertencentes ao mesmo grupo econômico detiver, também se submeterá.

O legislador elaborou tal redação com o intuito de por fim aos levantamentos trazidos por diversos provedores que não detêm representação da marca no Brasil, e utilizavam-se do argumento de não poder dispor dos dados de seus clientes uma vez que armazenados no exterior, exigindo-se por muitas vezes a expedição de carta rogatória para cooperação jurídica internacional entre os países envolvidos.

Além disso, procurou eliminar a questão societária evolvendo o tema, no que tange às empresas distintas pertencentes ao mesmo grupo econômico, sendo que apenas uma delas está sediada em terras nacionais. Nesta situação, havendo uma companhia presente no Brasil, integrante do mesmo grupo econômico do provedor responsável pelos dados requeridos, este também deverá obedecer às normas jurídicas brasileiras.

Trata-se de um ponto sensível, pois, caso não haja cumprimento por parte do provedor de determinado grupo econômico, localizado no exterior, de ordem de quebra de sigilo emanada por juízo brasileiro, a quem deverá ser determinada às sanções cabíveis? A empresa sediada no Brasil, porém não sendo responsável pela manutenção dos dados alvos da quebra e de que não detém qualquer controle dos dados exigidos? Ou há a possibilidade de punir a empresa estrangeira não sediada no Brasil, porém que conta com um de seus integrantes do grupo econômico ao qual pertence localizado em terras nacionais?

Por outro lado, ao realizar uma análise a luz do direito societário, é necessário ressaltar o princípio fundamental, que rege as relações de direito privado, da autonomia e independência das sociedades.

Nesse sentido, possível constatar que as pessoas jurídicas de direito societário conservam sua independência e autonomia mesmo que pertencentes a um mesmo grupo

econômico, uma vez que detêm personalidade e patrimônios distintos. Sendo assim, necessário se faz reconhecer a independência total das pessoas que constituem a sociedade.

Isto porque, cada pessoa jurídica que compõe um quadro societário possui determinada função social e econômica, de modo não pode assumir riscos e obrigações de outrem, alheios às suas atividades e diversas de seu objeto social, estando, portanto, impossibilitadas de responder por encargos e obrigações atinentes a outra sociedade.

Com efeito, salvo disposição contratual em contrário, o fato de sociedades membros do mesmo grupo econômico não as tornam corresponsáveis pelas obrigações umas das outras, seja em caráter solidário, ou subsidiário.

Desta forma, com relação às aplicações de sanções à empresa que teria descumprido ordem judicial, há ainda certa nebulosidade, o que dá margem a abusos das autoridades para se imporem perante essas companhias detentoras dos dados visados, para garantir o atendimento de suas solicitações[24].

Em se tratando de sanção, importante mencionar o artigo 12, do Marco Civil da Internet:

> Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:
>
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
>
> II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;
>
> III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou
>
> IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.
>
> Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o caput sua filial, sucursal, escritório ou estabelecimento situado no País.

[24] JESUS, Damásio E. de. **Marco civil da internet : comentários à Lei n. 12.965, de 23 de abril de 2014**. São Paulo Saraiva 2014 1 recurso online ISBN 9788502203200. p. 53.

Referido artigo dispões sobre penalidades a serem aplicadas aos provedores que não cumprirem o estipulado nos artigos 10 e 11, ambos do Marco Civil da Internet. Entretanto, há algumas peculiaridades na aplicação do supramencionado artigo aos casos concretos.

A problemática perante a qual nos deparamos, diz respeito sobre a aplicação destas sanções no âmbito criminal. O legislador não se preocupou em estabelecer como se dariam sua execução, quem seria competente em executá-la, em que momento, e qual seria o procedimento adequado.

Sendo assim, abre-se novamente margem à arbitrariedade estatal, uma vez que confere poderes amplos ao magistrado em fazer valer sua ordem de interceptação expedida.

Embasado na legitimidade conferida pelo artigo 12, a autoridade judiciária, ao determinar a quebra de sigilo telemática, de ofício já estabelece as penalidades a serem aplicadas em caso de descumprimento por parte dos provedores.

Muito comum, atualmente, acontecer de o juízo requisitante da quebra de sigilo, no âmbito criminal, no bojo de inquérito policial, como forma de coerção, ameaça a incidência de multa diária em caso de atraso no cumprimento, pelo provedor responsável pela manutenção dos dados alvo da interceptação.

Em seguida, diante do não atendimento de sua ordem, determina a aplicação e arbitramento do valor cumulado entre o recebimento do ofício pelo provedor até a atual data. Como se não bastasse, de plano exige-se seu pagamento, efetuando bloqueio dos ativos pertencentes a empresa, que, em tese, teria ignorado sua requisição.

Importa destacar que a multa estabelecida no artigo 12, do Marco Civil da Internet, não se trata de multa diária, e sim o arbitramento limitado até 10% (dez por cento) do faturamento econômico da companhia.

Nesse sentido, possível verificar que não há fundamento legal no ordenamento jurídico brasileiro no que tange a imposição de multa diária àquele que é terceiro, chamado aos autos para prestar esclarecimentos, no bojo de procedimento criminal. Em muitas decisões judiciais, a determinação da aplicação da penalidade é desacompanhada de seu respectivo fundamento legal, isto porque inexiste.

Não raras as vezes, o magistrado se utiliza de artigos oriundos do processo civil para embasar sua decisão, como os artigos 536, §1[25] e 537[26], ambos do Código de Processo Civil. Contudo, é cediço que a aplicação do processo civil no processo penal somente pode ser feita subsidiariamente, isto é, quando a lei processual penal não dispuser sobre o tema, conforme disposto no artigo 3, do Código de Processo Penal[27].

Ocorre que, a observância supletiva do Código de Processo Civil somente se viabiliza para preencher lacunas referentes aos princípios gerais no âmbito procedimental. Desta forma, inexequível a penalidade de cunho patrimonial em procedimento investigatório criminal, muito menos em face daquele que sequer está envolvido na investigação.

Isto porque as chamadas *astreintes* (multa diária) não têm aplicação ainda que por analogia em procedimento de investigação criminal, seja este de qualquer natureza (policial, parlamentar, ou de atribuição do Ministério Público).

Ainda, quanto a aplicação de sanções não especificadas na legislação penal, é possível encontrar magistrados que atuam na seara criminal, utilizando-se de seu poder geral de cautela para dar efetividade às suas decisões.

Neste aspecto, Aury Lopes Júnior leciona [28]:

> No processo civil, explica CALAMANDREI10, é reconhecido o poder geral de cautela (*potere cautelare generale*) confiado aos juízes, em virtude do qual eles podem, sempre, onde se manifeste a possibilidade de um dano que deriva do atra- so de um procedimento principal, providenciar de modo preventivo a eliminar o perigo, utilizando a forma e o meio que considerem oportunos e apropriados ao caso.

[25] "Art. 536. No cumprimento de sentença que reconheça a exigibilidade de obrigação de fazer ou de não fazer, o juiz poderá, de ofício ou a requerimento, para a efetivação da tutela específica ou a obtenção de tutela pelo resultado prático equivalente, determinar as medidas necessárias à satisfação do exequente.

§ 1o Para atender ao disposto no caput, o juiz poderá determinar, entre outras medidas, a imposição de multa, a busca e apreensão, a remoção de pessoas e coisas, o desfazimento de obras e o impedimento de atividade nociva, podendo, caso necessário, requisitar o auxílio de força policial."

[26] "Art. 537. A multa independe de requerimento da parte e poderá ser aplicada na fase de conhecimento, em tutela provisória ou na sentença, ou na fase de execução, desde que seja suficiente e compatível com a obrigação e que se determine prazo razoável para cumprimento do preceito."

[27] "Art. 3. A lei processual penal admitirá interpretação extensiva e aplicação analógica, bem como o suplemento dos princípios gerais de direito"

[28] JR., L. e Aury 2017, **Direito processual penal**, 14ª edição., 14th edição, Editora Saraiva. Disponível em: Minha Biblioteca. P. 584.

> Significa dizer que o juiz cível possui amplo poder de lançar mão de medidas de cunho acautelatório, mesmo sendo atípicas as medidas, para efetivar a tutela cautelar.
>
> (...)
>
> Mas isso só é possível no processo civil.
>
> No processo penal, não existem medidas cautelares inominadas e tampouco possui o juiz criminal um poder geral de cautela. No processo penal, forma é garantia. Logo, não há espaço para "poderes gerais", pois todo poder é estritamente vinculado a limites e à forma legal. O processo penal é um instrumento limitador do poder punitivo estatal, de modo que ele somente pode ser exercido e legitima do a partir do estrito respeito às regras do devido processo.

Neste diapasão, incontestável a inexistência de poder geral de cautela do juiz, referente às medidas cautelares atípicas no âmbito de procedimento criminal, tendo em vista que o poder conferido ao magistrado do juízo criminal se encontra vinculado à norma, não podendo se utilizar de medidas não previstas na legislação penal para garantia de suas exigências.

Por fim, retomando à questão da requisição de interceptação dos dados e comunicações telemáticas é possível constatar que a autoridade requisitante está vinculada à norma jurídica, devendo a determinação de quebra de sigilo conter alguns requisitos legais, quais sejam:

(i) ordem judicial devidamente fundamentada (e em casos de exceção, é dispensada a ordem judicial, cabendo ao Ministério Público ou Autoridade Policial de plano expedir as determinações de interceptação);
(ii) identificação clara e específica do conteúdo alvo da interceptação, para que o detentor dos dados, seja o provedor de conexão ou de aplicação, saiba exatamente qual o material apontado como infringente;

Diante de todo exposto ao longo deste capítulo, pode-se depreender que a proteção dos dados pessoais é a regra, e a interceptação presidida pelo Estado é a exceção, que se dá somente em situações específicas. A autoridade pública interessada nos dados deve, sempre quanto ao tratamento destas informações, atuar de acordo com as previsões e autorizações legais, respeitando também o princípio da proporcionalidade.

4- CRIPTOGRAFIA

Como forma de garantir a proteção aos usuários de internet foi desenvolvido um sistema de protocolos que impedem terceiros de lerem mensagens trocadas via internet, a chamada criptografia, que se trata de algoritmos criptográficos implementados em computadores.

O processo de cifragem envolve a conversão de um texto claro, ou seja, uma informação não cifrada, para um código cifrado. Isso impede o acesso por terceiros a conteúdo privado, garantindo que a informação cifrada esteja disponível apenas ao usuário.

Há dois tipos de criptografia atualmente[29]:

Criptografia simétrica, mais conhecida como de "ponta a ponta" (*end-to-end*), fundamenta-se em apenas uma única chave usada para ocultar certa informação, sendo essa mesma utilizada para revelar essa informação ao destinatário final. Sendo assim, somente os usuários tem acesso aos dados trocados entre si (utilizada pelo provedor de aplicação WhatsApp).

Criptografia assimétrica: diferentemente da simétrica, que envolve apenas uma chave, aqui existem chaves distintas que se complementam, o que torna mais difícil ainda o acesso por terceiros.

Sendo assim, uma vez que um terminal eletrônico encaminha conteúdo codificado, este, primeiramente, irá contatar os servidores do provedor da aplicação, que, por sua vez, irão encaminhar ao terminal destinatário, o qual receberá á chave decodificadora, para ter acesso ao conteúdo.

Dentro deste contexto, em momento algum, o provedor tem acesso ao teor do conteúdo das informações, uma vez que saem cifradas do terminal emissor, apenas sendo desencriptadas no receptor.

Nesse contexto, a interceptação telemática se dá quando é fornecida uma terceira chave à autoridade solicitante, que, a partir do momento em que é implementada, permite a

[29] ROHR, Altieres. **Criptografia: entenda o que é e como funciona**. Publicado em 2 de agosto de 206. Disponível em: http://g1.globo.com/tecnologia/blog/seguranca-digital/post/criptografia-entenda-o-que-e-e-como-funciona.html; Acesso em 8 de outubro de 2018.

replicação do conteúdo interceptado e sua decodificação. Vale ressaltar que somente será possível a duplicação do conteúdo enquanto esta chave adicional estiver implementada, isto é, mensagens anteriores a sua implementação e, após encerrada, não serão passíveis de interceptar.

Cumpre destacar que não necessariamente o titular do terminal interceptado é quem de fato redigiu a da mensagem ao receptor. Desta forma, pode-se dizer que descriptografia não é crucial para alcance do investigado.

Diante disso, as autoridades, mais especificadamente a policial, encontram barreiras para se inserir no meio virtual para obtenção de dados telemáticos, tendo em vista que, não raras vezes, ao efetuar solicitação de quebra de sigilo às empresas detentoras dos dados almejados, recebem resposta negativa, no sentido da impossibilidade em fornecê-los, oportunidade em que esclarece sobre a codificação.

Ocorre que, muitas vezes, essas autoridades não aceitam tal resposta e preferem embarcar em uma disputa com os provedores, seja instaurando inquérito para apurar crime de desobediência, por parte do representante da empresa (que na maioria das vezes não tem ciência do ocorrido e acaba sendo responsabilizado criminalmente), seja, em juízo, aplicando-se multa de altíssimos valores em face da empresa por suposto descumprimento de ordem judicial, quando não há bloqueio de ativos na conta da companhia, e dentre outras medidas abusivas tomadas por essas autoridades que custam a compreender a impossibilidade fática do fornecimento dos dados.

A despeito disso, vale citar a prisão do vice-presidente do Facebook do Brasil, em 1 de março de 2016, em decorrência de suposto descumprimento de ordem judicial que determinou a disponibilização de conteúdo de conversas entre usuários do aplicativo WhatsApp, suspeitos de utilizarem mencionado aplicativo para combinar práticas delitivas.

Isto porque, a referida empresa é detentora da maioria do aplicativo, o que justificou sua prisão.

Com efeito, é bastante comum autoridades alegarem que essas empresas fomentam as práticas delitivas em território brasileiro, cooperando para tanto. É inegável que o Judiciário pode se utilizar de métodos coercitivos a serviço do direito, mas não deveria fazê-lo para punir alguém por ter causado ranhuras em seu âmago.

Ora, o objeto social de uma empresa, e neste caso, das empresas de telefonia e tecnologia é a propagação de seu produto em território nacional, utilizando-se de meios legítimos para angariar clientes e desenvolver seus negócios. Alegar que estariam facilitando o cometimento de crimes quando não fornecem dados, em tese, armazenados em seu sistema, por não ser viável, profere tais afirmações em desacerto.

No âmbito internacional, têm sido reconhecidos os benefícios da criptografia. Dentro deste contexto, foi asseverado, ao longo do Fórum de Governança da Internet, evento organizado pela Organização das Nações Unidas (ONU), que esta codificação não acarreta em prejuízos ao combate à criminalidade[30].

Sem prejuízo, as autoridades têm exigido a criação de mecanismos decodificadores, para que tenham acesso ao conteúdo das mensagens privadas entre usuários.

Atualmente, há debates travados pelas autoridades policiais e jurídicas com as empresas de tecnologia e comunicação, acerca da legitimidade da criptografia.

Por um lado, argumenta-se que os princípios constitucionais não são revestidos de caráter absoluto, na medida em que a privacidade não pode ser utilizada para acobertar o cometimento de crimes.

Ainda, respaldado pelo Marco Civil da Internet, alega-se que a empresa que opera no Brasil, detentora de sede em território nacional, fica restrita à legislação brasileira, devendo se adequar aos ditames legais para o exercício de suas atividades.

Em contraponto, sustenta-se que não há qualquer regulamentação, tanto no âmbito nacional quanto internacional sobre a proibição de criptografar conteúdos, ou que obrigue os provedores a implementarem mecanismos decodificadores para revelar a terceiros o conteúdo de mensagens trocadas entre usuários.

---

[30] GROSSMANN, Luís Osvaldo. **Era de ouro da vigilância**. Publicado em 10 de novembro de 2015. Disponível em: http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=41088&sid=4; Acesso em 10 de outubro de 2018.

Sendo assim, não há de ser considerada como ilícita a atividade desenvolvida por tal empresa, uma vez que ninguém se torna obrigado a fazer ou deixar de fazer algo senão em virtude de lei[31].

Ainda, não se pode obrigar a pessoa física ou jurídica ao cumprimento de ordem judicial, cuja obrigação de fazer é impossível, dada a inviabilidade técnica, muito menos exigir que a pessoa jurídica passe a desenvolver estrutura para que possa atender a demanda exigida pelo judiciário brasileiro, sendo que esta estrutura é custosa e prejudicial para o caminhar dos negócios. Ainda mais em um país cuja burocracia e os custos para gerir uma sociedade empresarial são altos, colocar mais uma exigência seria barrar seu desempenho no país.

Além disso, importa salientar que a criptografia não tem como finalidade dificultar o deslinde de investigações, pelo contrário, é um método para garantir a privacidade das informações ante um mundo globalizado e altamente conectado.

Trata-se, portanto de padrão de segurança obrigatório, sendo uma medida de proteção para garantir a inviolabilidade dos dados, consoante com determinação expressa no artigo 13, inciso IV, do Decreto n. 8.771 de 2016[32], que regulamenta a Lei Federal n. 12.965 de 2014 (Marco Civil da Internet).

> Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança:
>
> (...)
>
> IV – o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes.

Neste contexto, havendo regulamentação determinando a obrigatoriedade de se estabelecer estruturas de preservação da intimidade dos usuários da rede, isto é, expressa lei

---

[31] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
II - ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei;

[32] BRASIL. **Decreto n. 8.771 de 2016**. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm. Acesso em 03 de outubro de 2018.

que incentiva o uso da criptografia, não cabe ao Poder Judiciário se opor a mesma, tomando decisões de forma contrária.

Ademais, a controvérsia que envolve esta questão é tema de debate perante o Supremo Tribunal Federal, no bojo de Ação Declaratória de Preceito Fundamental (ADPF n. 403), bem como de Ação Direta de Inconstitucionalidade (ADI n. 5527).

Neste cenário, em decorrência da necessidade de maiores esclarecimentos técnicos a respeito da controvérsia discutida, foi realizada audiência pública. Naquela oportunidade foram realizadas exposições de técnicos do assunto.

Assim, dentre os principais temas explorados, foram esclarecidos os seguintes pontos: (i) impossibilidade de obter teor das mensagens já transmitidas pelo aplicativo WhatsApp; e (ii) inserir falha proposital ao protocolo de segurança para garantir a interceptação das mensagens torna o sistema menos seguro, e mais caro de sustentar, e, como consequência, estimula a migração dos usuários para outros aplicativos que garantam maior segurança de suas informações.

Sendo assim, a discussão acerca da necessidade de descodificação de mensagens criptografadas ainda está no longe de ser pacífica no Brasil, na medida em que está permeada por questões técnicas complexas, estando pendente a manifestação do Egrégio Supremo Tribunal Federal sobre a legalidade da criptografia.

Com efeito, "É importante esclarecer que nunca foi tão fácil monitorar a sociedade e está cada vez mais difícil o isolamento digital e o bloqueio da comunicação (*go dark*)."[33]

Estamos diante de uma era em que temos que zelar pelo mínimo de intimidade que nos resta. É evidente que não é necessário nos despirmos das tecnologias que temos a nossa disposição. Mas ao ter ciência sobre a possibilidade de estar sendo monitorado cem por cento do tempo, temos que nos utilizar do mínimo de segurança que é proporcionada.

O *The New York Times* publicou uma matéria, em 2013, na qual revelava que a *National Security Agency* (N.S.A.) se utilizava de supercomputadores e técnicas persuasivas para burlar as principais ferramentas de proteção da privacidade das comunicações, tanto

[33] CHACON, Eduarda. **Encriptação e acesso judicial**. Publicado em 22 de março de 2016. Disponível em: https://www.migalhas.com.br/dePeso/16,MI236262,81042-Encriptacao+e+acesso+judicial. Acesso em 03 de outubro de 2018.

americanas, quanto internacionais[34]. Dados como relatórios médicos e segredos comerciais, eram alvos da agência, além de burlar sistemas bancários e comerciais.

Segundo o artigo, N.S.A. desenvolveu métodos para obtenção da informação antes mesmo que fosse criptografada. Em alguns casos, as empresas detentoras dos dados alegavam que eram coagidas a fornecerem tais informações à agência.

Se tal burla ocorreu em 2013, quiçá passados cinco anos.

Os usuários da rede confiam às empresas com as quais contratam suas informações pessoais, e esperam como retorno um tratamento dos dados seguro e controlado. Desta forma, a criptografia é essencial para garantir a proteção do usuário, além de permitir que este se sinta inserido em um meio menos monitorado, se comparado com o qual já vive.

Pode-se dizer que se trata de uma batalha na qual as autoridades tenham esperança de criar um pretexto para ajustar a iniciativa privada aos interesses de vigilância do governo na área da tecnologia, ao se impor de tal maneira[35].

Fato que deveria ser o oposto, sendo que o Estado tem que se amoldar à sociedade perante a qual tenta se impor. Travar disputas com as empresas de telefonia e tecnologia não assegura o alcance da real finalidade, qual seja, chegar a um indivíduo que supostamente cometeu algum crime. Pelo contrário, apenas o desvirtua.

Nesse aspecto, é importante que as autoridades e essas empresas caminhem juntas, cooperando umas com as outras, para que não haja empasses quando estiverem diante de problemas, para que soluções sejam alcançadas de forma pacífica e seja efetivada a investigação criminal e a persecução penal.

Outro ponto, muito comum, é que, em variadas situações, a autoridade expede ofício determinando a quebra de sigilo para o detentor dos dados, que, por sua vez, responde pela ausência de dados, esclarecendo seus motivos. Em paralelo, esta mesma autoridade realiza atos

---

[34] PERLROTH, Nicole; LARSON, Jeff; SHANE, Scott. ***N.S.A. Able to foil basic safeguards of privacy on web***. Publicado em 5 de setembro de 2013. Disponível em: https://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html. Acesso em 12 de julho de 2018.

[35] CHACON, Eduarda. **Encriptação e acesso judicial**. Publicado em 22 de março de 2016. Disponível em: https://www.migalhas.com.br/dePeso/16,MI236262,81042-Encriptacao+e+acesso+judicial. Acesso em 03 de outubro de 2018.

diversos tão passíveis de se chegar ao investigado, quanto à quebra de sigilo em questão, sendo que, em não raras situações, acaba por descobrir quem é o suspeito e sua localização, e ainda prefere insistir na quebra de sigilo, ou na aplicação de sanções em face do alegado "descumprimento".

Neste cenário, Eduarda Chacon pontua acertadamente[36]:

> O desafio é que a regulação da internet é muito complicada, na medida em que não pode ser excessiva ou restritiva demais sob pena de confinar o desenvolvimento da rede. Além disso, a complexidade da elaboração das políticas públicas legais permeia um limite tênue entre segurança e privacidade, especialmente na questão atinente aos dados criptografados ou protegidos por encriptação de hardware.
>
> A legislação, deste modo, precisaria definir muito claramente quem poderia ser solicitado a auxiliar, perante quais autoridades e de que modo, sob quais especificidades, quais detalhamento de forma, parâmetros e circunstância, e quais critérios mínimos justificariam uma intervenção via ordem judicial no caso concreto.
>
> Observe-se que somente em relação aos dados criptografados armazenados em um gadget, existem pelo menos três ângulos, nenhum deles abordado pela legislação: (i) o acesso a conteúdo decodificado de conversa cifrada (plaintext) travada por meio de app, como ocorre com o WhatsApp e IMessage; (ii) a superação do password e quebra das chaves de encriptação do hardware de um celular específico, o que ninguém sabe como fazer, e (iii) a criação de backdoor com potencial para atingir bilhões de usuários, como sugere o FBI no caso San Bernardino.

Por fim:

> "A internet é o palco se desenrola a trama da luta contra a criptografia e o espectador está sendo induzido a acreditar que existem apenas dois lados: apoiá-la para defender a privacidade ou combatê-la para enfrentar o cyber terrorismo. A verdade é que raramente as coisas são simples como o preto ou branco; é preciso buscar meios de equilibrar as aparentes contradições e oferecer respostas, em uma realidade cinzenta, que ultrapassem a retórica em prol das soluções válidas."

[36] CHACON, Eduarda. **Encriptação e acesso judicial**. Publicado em 22 de março de 2016. Disponível em: https://www.migalhas.com.br/dePeso/16,MI236262,81042-Encriptacao+e+acesso+judicial. Acesso em 03 de outubro de 2018.

5- METODOLOGIA DE INVESTIGAÇÃO DE CRIMES CIBERNÉTICOS

É notória a prática delitiva em meios eletrônicos. Atualmente, a rede é utilizada tanto como fim, quanto como meio para o cometimento de crimes, isto é, há a consumação de delitos na própria internet, a exemplo, crimes contra honra, bem como muitos dos atos preparatórios são realizados na internet, como tráfico de pessoas, ou seja, consuma-se no mundo real, porém o restante é elaborado na própria internet.

Ante aos incontáveis crimes praticados por meios eletrônicos, precisou-se desenvolver métodos para se alcançar aqueles que os realizam. Para tanto, em regra, o mais importante é saber o terminal originário do conteúdo criminoso, ou da prova.

O artigo 5, da Lei 12.965 de 2014, conceitua terminal como qualquer dispositivo que se conecta a internet. Sendo assim, qualquer aparelho passível de se conectar à rede informatizada é considerado como terminal.

Com efeito, para descobrir qual o terminal deu origem ao conteúdo alvo da investigação, é preciso realizar alguns passos.

Em primeiro lugar, identificar o meio em que o crime foi cometido, seja em um website, e-mail, páginas de relacionamento, programas de mensagens instantâneas, e dentre outros, de modo para que saiba quem é detentor das informações do usuário responsável pelo conteúdo investigado.

Sendo assim, uma das mais importantes evidências a ser coletada é o endereço de protocolo de internet, mais comumente conhecido como registros de IPs (*Internet Protocols*), o qual se trata de um código identificador atribuído a um terminal conectado à internet, definido segundo parâmetros internacionais (encontra-se no formato A.B.C.D, onde cada letra são codificadas por números que variam de 0 (zero) a 255 (duzentos e cinquenta e cinco).

Para melhor auxílio com a investigação, essencial que o IP venha acompanhado pela data e hora da conexão ou comunicação e o fuso horário do sistema.

Nesse diapasão, necessário se faz trazer os conceitos estabelecidos pelo Marco Civil da Internet para melhor clareza dos termos. Temos, então, os chamados registros de conexão, os quais se tratam de "(...) 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

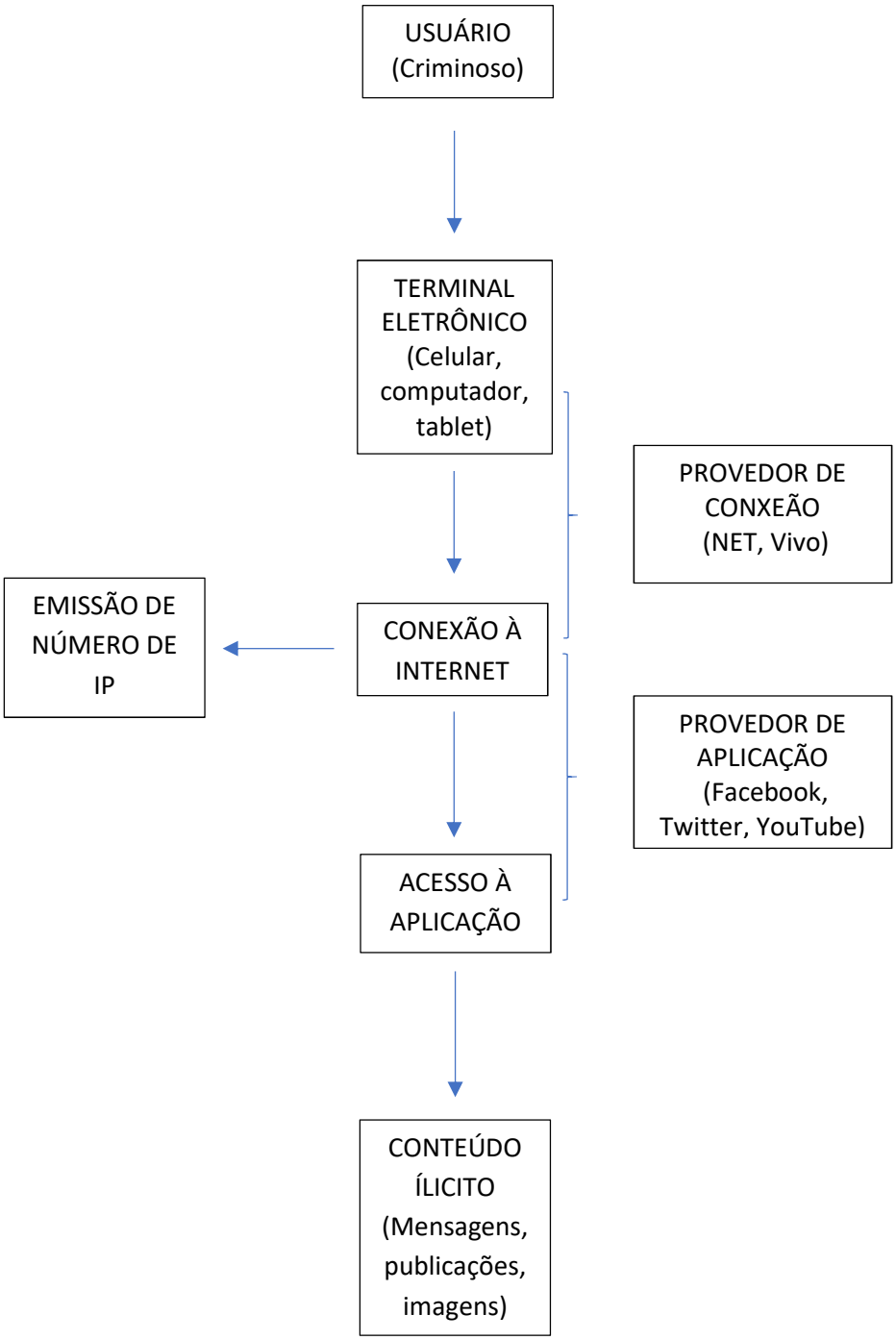
recebimento de pacotes de dados.”; e os registros de aplicação, que envolvem um conjunto de informações sobre o uso de determinada aplicação a partir de um certo IP[37].

Então, como exemplo, utilizaremos um caso de venda de moeda falsa através de rede de relacionamento virtual. Como primeira diligência será identificar o meio, e, como vimos, trata-se de uma aplicação na internet. Em seguida, será necessária a requisição dos registros de aplicação ao provedor de aplicação responsável pelo seu armazenamento.

Com base nessas informações, serão verificadas qual foi o provedor de conexão que forneceu acesso ao terminal eletrônico à internet, e requisitar as informações necessárias para a elucidação dos fatos, com relação ao IP alvo.

Sendo assim, será possível identificar onde está localizado o terminal e quem é seu proprietário. Para facilitar a compreensão, temos:

[37] BRASIL, **Lei n. 12.965**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 03 de outubro de 2018



Em outras palavras, fazendo o caminho inverso, ao detectar o conteúdo ilícito, disponível em uma aplicação (sites de navegação), determina-se a quebra de sigilo dos dados telemáticos, direcionado ao provedor de aplicação, que, por sua vez, encaminhará o IP que deu origem a este conteúdo, bem como data e hora de seu registro.

Com base neste IP, será possível detectar qual o provedor de conexão é responsável pelo seu registro, devendo haver nova quebra, buscando-se informações acerca do cliente que contratou com a empresa, originário do endereço de protocolo de internet.

6- CONCLUSÃO

As conclusões a que se chegou no decorrer desta pesquisa foram expostas ao longo deste trabalho.

Conforme se infere da leitura do primeiro capítulo, é feita uma abordagem sobre a proteção à intimidade, privacidade e confidencialidade das comunicações na Constituição Federal de 1988, inserida no artigo 5º, da Lei Maior, sendo este classificado como cláusula pétrea, de proteção máxima, conferida pela própria Carta Magna.

No que tange a questão da abrangência da aplicação do princípio de inviolabilidade das comunicações, há entendimentos de que somente são abarcadas as informações referentes às comunicações dos usuários na internet. Contudo, adota-se o posicionamento que os dados relacionados aos registros de acesso e conexão à internet, bem como aqueles fornecidos pelos próprios internautas ao efetuar o se conectar a um determinado domínio.

Em seguida, no segundo capítulo, é realizado um estudo sobre a legislação que regula a interação dos usuários na internet e dos provedores de aplicação e conexão, a Lei 12.965 de 2014. Sendo assim, possível constatar que a autoridade requisitante da interceptação telemática está vinculada à norma jurídica, devendo a requisição de quebra de sigilo conter os requisitos legais, quais sejam: ordem judicial devidamente fundamentada e identificação clara e específica do conteúdo alvo da interceptação, para que o detentor dos dados saiba exatamente qual o material apontado como infringente.

Como problemática, foi abordado neste trabalho de conclusão de curso o tema da legalidade da criptografia, como meio de proteção dos dados informáticos, uma vez que se trata de uma barreira para a violação do sigilo das comunicações nos casos de investigação criminal e a persecução penal.

Com base nas pesquisas feitas, embora ainda pendente decisão no STF acerca desta questão, é reconhecida a importância desta ferramenta para a preservação da intimidade da vida privada dos usuários da rede, diante da constante exposição que sofrem por estarem inseridos neste meio, bem como da ausência de controle daquilo que é monitorado.

Embora a desencriptação seja um meio mais certeiro para se alcançar o investigado, ou para obter as provas necessárias para a conclusão da investigação ou instrução, e que a

criptografia prejudica a ação da autoridade policial e do Ministério Público na apuração dos fatos, conclui-se que devidamente em consonância com o ordenamento jurídico brasileiro, não devendo ser considerada ilegal, por ser um dos instrumentos mais seguros e aptos para garantir a manutenção da confidencialidade dos dados telemáticos e, mais especificamente, das comunicações pessoais.

Por fim, em decorrência dos inúmeros delitos cometidos na internet e a necessidade de se obter maiores informações possíveis para auxiliar na perquirição dos fatos, importante que se detenha certo conhecimento do funcionamento da rede, os métodos adotados para obter essas informações, e depois que obtidas, como utilizá-las.

Para tanto, o último capítulo foi dedicado a exposição dos passos a serem adotados para o alcance da verdade real. Sabe-se que na prática muitos outros empecilhos podem ser encontrados ao longo do caminho, mas, uma vez dominando os procedimentos adequados, será possível atingir a finalidade almejada de forma célere e certeira.

7- REFERÊNCIAS BIBLIOGRÁFICAS

Livros

ALEXY, Robert. **Teoria dos direitos fundamentais**. 2. ed. São Paulo: Malheiros, 2011. 669 p. (Teoria & direito público) ISBN 9788539200733

CHACON, Eduarda. **Encriptação e acesso judicial**. Publicado em 22 de março de 2016. Disponível em: https://www.migalhas.com.br/dePeso/16,MI236262,81042-Encriptacao+e+acesso+judicial. Acesso em 03 de outubro de 2018.

DEZEM, Guilherme Madeira. **Curso de processo penal**. 3. ed., rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2017. 1279 p. ISBN 9788520370797

FERRAZ JUNIOR, Tércio Sampaio. **Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado**. Cadernos de Direito Constitucional e Ciência Política, São Paulo, no 1, 1998

GOMES, Luiz Flávio. **Interceptação telefônica: lei 9.296, de 24.07.1996**. São Paulo: Revista dos Tribunais, 1997. 278 p. ISBN 8520314996

HOESCHL, Hugo Cesar. **O tratamento normativo da telemática no Brasil**. Florianópolis: Ijuris, 2000.

JESUS, Damásio E. de. **Marco civil da internet : comentários à Lei n. 12.965, de 23 de abril de 2014**. São Paulo Saraiva 2014 1 recurso online ISBN 9788502203200.

JR., L. e Aury 2017, **Direito processual penal**, 14ª edição., 14th edição, Editora Saraiva. Disponível em: Minha Biblioteca.

LEITE Salomão, G. Lemos e R.(Coord.). 09/2014, **Marco Civil da Internet**, Atlas. Disponível em: Minha Biblioteca.

MARCO civil da internet. São Paulo Atlas 2014 1 recurso online ISBN 9788522493401.

MASSO, Fabiano Del; ABRUSIO, Juliana Canha; FLORÊNCIO FILHO, Marco Aurélio (Coord.). **Marco civil da internet: lei 12.965/2014**. São Paulo: Revista dos Tribunais, 2014. 268 p. ISBN 9788520353066

PAESANI e , L.M. 10/2014, **Direito e Internet: Liberdade de Informação, Privacidade e Responsabilidade Civil***, 7ª edição*, Atlas. Disponível em: Minha Biblioteca.

PERLROTH, Nicole; LARSON, Jeff; SHANE, Scott. ***N.S.A. Able to foil basic safeguards of privacy on web***. Publicado em 5 de setembro de 2013. Disponível em: https://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html. Acesso em 12 de julho de 2018.

RODRIGUEZ, Victor Gabriel. **Tutela penal da intimidade: perspectivas da atuação penal na sociedade da informação**. São Paulo: Atlas, 2008 xii, 261 p. ISBN 9788522450848

SCORSIM, Ericsom M. **A questão da criptografia do WhatsApp: julgamento do caso pelo STF sob a perspectiva da segurança das comunicações**. Publicado em 6 de junho de 2017. Disponível em: https://www.migalhas.com.br/dePeso/16,MI259918,71043-A+questao+da+criptografia+do+WhatsApp+julgamento+do+caso+pelo+STF+sob. Acesso em 4 de outubro de 2018.

SILVA, R. S. M. **A interceptação das comunicações telemáticas no processo penal**. 266 f. Dissertação (mestrado) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2014.

SYDOW, Spencer Toth. **Crimes informáticos e suas vítimas**. 2. São Paulo Saraiva 2014 1 recurso online (Saberes monográficos). ISBN 9788502229495.

Legislação

BRASIL, **Código Penal**. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em:

BRASIL, **Constituição Federal de 1988**. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 03 de junho de 2018.

BRASIL, **Código de Processo Penal**. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm. Acesso em: 09 de outubro de 2018;

BRASIL, **Código de Processo Civil**. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em 9 de outubro de 2018;

BRASIL. **Decreto no 678, de 1992 (promulgação):** Convenção Americana sobre Direitos Humanos [anexo]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/D0678.htm. Acesso em: 02 de outubro de 2018;

BRASIL. **Decreto n. 8.771 de 2016**. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm. Acesso em 03 de outubro de 2018;

CIDH. **Declaração Americana dos Direitos e Deveres do Homem**. Bogotá, abr. 1948. Disponível em: http://www.direitoshumanos.usp.br/index.php/OEA-Organiza%C3%A7%C3%A3o-dos-Estados-Americanos/declaracao-americana-dos-direitos-e-deveres-do-homem.html Acesso em: 02 de outubro de 2018;

NAÇÕES UNIDAS. **Declaração Universal dos Direitos do Homem**. Disponível em: https://www.unicef.org/brazil/pt/resources_10133.htm Acesso em: 02 de outubro de 2018;

BRASIL, Lei n. 12.683. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12683.htm. Acesso em 5 de outubro de 2018;

BRASIL, **Lei n. 12.737 de 2012**. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm. Acesso em 4 de junho de 2018.

BRASIL, **Lei n. 12.850**. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm. Acesso em: 05 de outubro de 2018;

BRASIL, **Lei n. 12.965**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 03 de outubro de 2018;

BRASIL, **Lei n. 13.260**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13260.htm. Acesso em 5 de outubro de 2018;

BRASIL, **Lei n. 13.709 de 2018**. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em 08 de outubro de 2018.

Jurisprudência

STJ. RMS n.º 56.706/RS. Rel. Ministro Felix Fischer. Quinta Turma. DJe 09.05.2018.

STJ. RHC 75.055/DF. Rel. Ministro Ribeiro Dantas, Quinta Turma. DJe 27/03/2017.