UNIVERSIDADE PRESBITERIANA MACKENZIE

MOHAMAD HASSAN FARES

QUEBRA DE SIGILO TELEMÁTICO

SÃO PAULO

2019

MOHAMAD HASSAN FARES

QUEBRA DE SIGILO TELEMÁTICO

Trabalho de Conclusão de Curso apresentado à Universidade Presbiteriana Mackenzie do Estado de São Paulo como requisito parcial à obtenção do grau de Bacharel em Direito.

Orientador: Prof. Dr. Marco Aurélio Florêncio Filho

SÃO PAULO

2019

FARES, Mohamad Hassan.

QUEBRA DE SIGILO TELEMÁTICO.

Trabalho de Conclusão de Curso para obtenção do grau de Bacharel em Direito – Universidade Presbiteriana Mackenzie, Cidade e Estado de São Paulo, 2019.

1. Quebra de Sigilo Telemático. 2. Medida Cautelar. 3. Dados Armazenados. 4. Interceptação de Comunicação Telemática.

MOHAMAD HASSAN FARES

QUEBRA DE SIGILO TELEMÁTICO

Trabalho de Conclusão de Curso apresentado à Universidade Presbiteriana Mackenzie do Estado de São Paulo como requisito parcial à obtenção do grau de Bacharel em Direito.

Aprovado em:_____/_____/_____.

BANCA EXAMINADORA:

_____

Prof. Doutor Marco Aurélio Florêncio Filho

_____

Prof. Avaliador: Fábio Ramazzini Bechara

_____

Prof. Avaliador: Gabriel Druda Deveikis

A Deus, que sempre me proporcionou tudo do bom e do melhor na vida. Sem Ele, eu nunca teria me tornado no ser humano que me tornei.

AGRADECIMENTOS

Quero agradecer e dedicar esta dissertação à seguintes pessoas:

À minha mãe, por todo seu suporte e por tudo que a senhora largou mão na sua vida para ficar comigo e com meu irmão. Pelo amor incondicional que nós temos um pelo outro.

Ao meu pai, que, independentemente de qualquer situação, sempre esteve ao meu lado, me apoiando e ajudando em tudo que eu precisasse. O homem mais forte que eu conheço.

Ao meu irmão, meu melhor amigo e parceiro. Não sei o que seria de mim sem você.

A toda minha família.

A minha grande amiga Ariadne, por tudo que você me ensinou e ensina, seja com críticas ou com seu suporte. Você foi fundamental no momento mais importante da minha vida profissional e pessoal. Palavras não são suficientes para dizer o quanto eu sou grato por tudo.

A todos do então escritório Sica e Quito. Sem exceção. Os ensinamentos que lá aprendi, carregarei pelo resto da minha vida.

A todos meus amigos, mas, principalmente, ao Gabriel Angelieri, Guilherme Canedo, Tiago Macedo, Gabriel Pancha, Eric de Mello, Philippe Hlinsky, Fares Naceibe Fares, Tarik Zohbi, Majd Marjoub, Danielle Brancolini, Bruno Vitti e Vitória Tedeschi.

RESUMO

O presente trabalho tratou de abranger dois aspectos de meio de obtenção de prova em inquéritos e ações penais, no processo penal vigente no país. Trata-se da quebra de sigilo telemático que dividimos em (i) busca e apreensão dos dados armazenados e (ii) interceptação de comunicação. Para tanto, explicamos os tipos de dados existentes no mundo telemático e quais desses estão previstos no Marco Civil da Internet e quais estão sujeitos à Lei de Interceptação Telefônica.

Deste modo, procuramos, em ordem cronológica à data da decisão de quebra de sigilo, enumerar certas possibilidades do que pode vir a ocorrer em razão desta, e, posteriormente, separar os tipos de dados existentes e aplica-los nas respectivas leis que os abrangem, e, por fim, apontando uma lacuna na legislação no que se refere à interceptação de dados diversos de comunicação.

Palavras-chave: Quebra de Sigilo Telemático. Marco Civil da Internet. Interceptação Telemática. Dados armazenados. Comunicação humana.

ABSTRACT

The present academic work seeks to contribute to the study of breach of secrecy at a crime process in Brazil. For this, we have separated this institute in 2: (i) stored content and (ii) future content (wiretapping of e-mails). We had explained that there are a lot of data, and those data's are classified due the law, so the stored content could be applied by the "busca e apreensão" methode, and the future content of communication, necessarily, should be applied by the "Lei de Interceptação Telefônica e Telemática".

So we could make this work, we had explained the data`s that the Brazilian law covers, and individualized each one as a determined group of data, so they could be peaceful of a legal breach of secrecy by a judge decision.

Keywords:. Breach of Secrecy. Marco Civil da Internet. Wiretapping. Store content. Future Content.

Sumário

INTRODUÇÃO *10*

1. Valores Processuais *12*

1.1 A BUSCA DA VERDADE NO PROCESSO PENAL 12

1.2 INQUÉRITO POLICIAL 13

1.3 PROVAS 14

1.4 MEIOS DE PROVA E MEIOS DE OBTENÇÃO DE PROVA 15

1.5 PRESSUPOSTOS PARA A REQUISIÇÃO DA QUEBRA DE SIGILO 17

1.6 LEGITIMIDADE 18

1.7 A AUTORIZAÇÃO JUDICIAL PARA A QUEBRA DE SIGILO 21

1.8 O PROCESSAMENTO DA ORDEM PELO PARTICULAR 23

1.9 DAS HIPÓTESES QUE PODEM SURGIR APÓS A COMUNICAÇÃO DA QUEBRA DE SIGILO 24

2. MODALIDADE DE DADOS *26*

2.1 DADOS CADASTRAIS 26

2.2 DADOS DE TRÁFEGO 27

2.3 COMUNICAÇÃO HUMANA 29

2.4 DADOS DIVERSOS DE COMUNICAÇÃO 30

3. DOS MEIOS DE OBTENÇÃO DE PROVA *30*

3.1 BUSCA E APREENSÃO 30

3.2 INTERCEPTAÇÃO DA COMUNICAÇÀO TELEMÁTICA 35

3.3 INTERCEPTAÇÃO DE DADOS DIVERSOS DE COMUNICAÇÃO 39

Conclusão *44*

Referencias Bibliográficas *46*

INTRODUÇÃO

A presente monografia versa sobre a Quebra de Sigilo Telemático no Processo Penal. Trata-se de uma medida cautelar que poderá ser decretada no bojo de inquéritos policiais e ações penais, como meio de obtenção de prova, sendo um procedimento sigiloso e que terá como objeto, a quebra do sigilo de dados telemáticos, bem como a comunicação telemática das pessoas que interessam à ela.

Tema novo e de suma importância para as autoridades inquisitórias obterem informações importantes acerca dos crimes a serem apurados, e que, cada vez mais, terá uma gama ainda maior de informação pelos Provedores de Rede e de Conexão a serem fornecidos, mediante ordem judicial. Com o crescimento exponencial de produtos e serviços disponíveis aos usuários da internet, o acesso às informações pessoais é de extrema necessidade e importância para quem investiga, pois com base nesses dados, a probabilidade de se confirmar a autoria de um crime ou encontrar novas provas sobre o que está sendo investigado, é muito maior. Apesar disso, deve-se verificar todos os limites impostos não apenas pelas Leis que regem o tema, mas também pela Constituição Federal, já que esta lista os direitos fundamentais do ser humano, impondo limites para o processo penal democrático.

O presente estudo foi realizado com base em doutrinas de processo penal, de direito constitucional e em doutrinas que estudam a Lei 9.296/96, que trata sobre as interceptações telefônicas, telemáticas e telegráficas, bem como da Lei Federal 12.965/14. Com base neles, conseguimos, de forma didática, destrinchar os meios de obtenção de provas que são obtido mediante uma quebra de sigilo telemático, onde, justamente por ser um tema recente, muitas vezes ainda passa despercebido dos órgãos inquisitivos e do Poder Judiciário, de forma geral.

Em um primeiro momento, analisamos os pré-requisitos para que seja possível a decisão da medida cautelar. Destacamos os pontos intrínsecos à medida, como os legitimados a requerem, a necessidade de ordem judicial, do requisito específico da Lei 9.296/96 (sua aplicabilidade incide apenas para crimes apenados com reclusão), o valor da prova obtida mediante a quebra de sigilo e como deverá ser realizado o processamento da ordem pelo particular, bem como sua legitimidade em impugnar decisões iligais.

No segundo momento da presente monografia, procuramos distinguir os tipos de dados existentes, para que, depois, pudéssemos aplica-los perante as leis vigentes. São eles: (i) dados cadastrais; (ii) dados de tráfego; (iii) comunicação humana; e (iv) dados diversos de comunicação.

A diferenciação desses dados é da máxima importância, pois nem todos são aplicáveis a lei de interceptação telemática, por exemplo, como explicamos, por fim, no capítulo 3 da presente. Mostraremos como os dados devem ser fornecidos, as peculiaridades (leia-se lacuna) na lei, e o dever de não ser cumprida ordens judiciais manifestamente ilegais, nas quais não respeitam os limites impostas pelas Leis ou, desrespeitando, em níveis desproporcionais, a esfera intima e privada do sujeito alvo da medida.

1. Valores Processuais

1.1 A BUSCA DA VERDADE NO PROCESSO PENAL

Não existem direitos fundamentais absolutos. A função do Estado não é proteger esses direitos, e sim de assegurar que você os possua, e que, quando for necessário e de interesse público, o Estado intervirá nesses direitos, para garantir que ele não está sendo utilizado de forma exorbitante. Por consequência, entendemos que nenhum direito fundamental é absoluto.

Assim, conseguimos entender que os direitos consagrados na Constituição Federal, que disciplina a inviolabilidade da intimidade e da vida privada[1], bem como o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas[2], poderão ser afastados com a necessidade da aplicação da força Estatal, sempre sendo aplicada de maneira proporcional. De um lado, o Estado possui o direito de punir alguém, e de outro, o dever de assegurar os direitos da pessoa.

A fase investigatória de uma persecução penal tem como finalidade, segundo a leitura do art. 4º do Código de Processo Penal, a apuração das infrações criminais e de sua autoria. Esse procedimento administrativo é regido por direitos e limites, já que estamos falando de um instrumento estatal que irá afrontar direitos fundamentais, como a inviolabilidade de sigilo. Segundo Gustavo Badaró[3], "trata-se de um procedimento na medida em que o legislador prevê uma sequência de atos praticados, pela autoridade policial, prevendo os meios de início, quais as diligencias serem realizadas, a forma dos atos investigatórios, o prazo, e o término do inquérito policial."

Para Tourinho Filho[4] a verdade formal deve ser construída conforme a constante incerteza do juiz. Ele não deve se contentar com o que as partes produziram, mas sim como que o crime ocorreu, em todas as suas circunstâncias, para assim, contruir sua convicção e dar base a mais digna Justiça.

---

[1] Art 5º, X da Constituição Federal.
[2] Art. 5º, XII da Constituição Federal
[3] BADARÓ, Gustavo. Processo Penal. São Paulo: Revista dos Tribunais. 2015. p. 116.
[4] TOURINHO FILHO, Fernando da Costa. Processo Penal, volume 1. São Paulo: Saraiva. 2010. p. 59.

É nessa fase pré-processual onde irão ser reunidas o máximo de elementos probatórios possíveis que permitem a busca da verdade para que futuramente seja viabilizado a fase de persecução penal em juízo".

Com efeito, conseguimos entender que a busca da verdade real dar-se-á pelo fato de o juiz não se contentar com verdade inserida nos autos de um processo-crime, mas sim de sempre buscar pelos meios legais disponíveis a maior proximidade possível da verdade real, o que de fato ocorreu na situação fática material, e que eventualmente, não está inserida nos autos do processo. Para que o juiz a alcance, contudo, deve-se respeitar os limites decorrentes da Lei, das quais a Constituição Federal e as Leis infraconstitucionais impõe para que seja assegurado os direitos do réu e de sua defesa, do Ministério Público e da autoridade policial, bem como de uma sociedade toda.

A partir do entendimento que será preciso a maior proximidade dos fatos para a justa causa da ação penal, e traçando um paralelo com a quantidade de informação que depositamos ou que são geradas, diariamente, direta e indiretamente, intencionalmente ou não, nos nossos dispositivos eletrônicos, extraímos a grande importância de como a quebra de sigilo telemático se tornou de suma importância para os órgão inquisitivos. Embora a facilidade e a montanhosa quantidade de informações que são possíveis de se obter requisitando e obtendo dados privados de uma pessoa na seara digital, o Estado deve observar determinados limites à sua atuação no que se refere às interferências na vida dos indivíduos, na sua intimidade e privacidade, quando estiver buscando a reconstrução histórica de um fato criminoso[5].

1.2 INQUÉRITO POLICIAL

O Inquérito tem como finalidade apurar fato que constitui infração penal e de sua possível autoria. Note que o inquérito não traz a certeza de que o suposto autor cometeu a infração penal, mas sim que pelos elementos colhidos durante o procedimento, criou-se um juízo de probabilidade para que àquele(s) que foram identificados possam ou não responder um processo crime pela sua atividade (seja como autor ou partícipe) na infração penal.

Durante o inquérito, tem-se por finalidade reunir os elementos probatórios após as diligências realizadas pela autoridade policial (inquisitiva), e aquelas requeridas pelo

[5] SIDI, Ricardo. A interceptação das comunicações telemáticas no processo penal. Belo Horizonte: D'Plácido. 2016. p. 75.

Promotor de Justiça (em casos de ação penal pública), para se aproximar da já dita verdade real, e sendo o caso, ser recebida a denúncia ofertada pelo Ministério Público ou o mesmo requerendo o arquivamento do procedimento inquisitivo por falta de elementos suficientes para que o investigado se torne réu em uma ação penal. Tais diligências são de extrema importância para a colheita de provas, já que são com elas reunidas nos autos que a verdade formal será exposta e ao juiz, que pode decidir para o início da ação penal ou não diante do convencimento de indícios suficientes de autoria.

Importante ressaltar que as provas colhidas no inquérito não poderão ser utilizadas como única fonte para que o juiz condene o réu. Essas provas, obtidas na fase pré processual, não garantem o contraditório para o investigado, visto que apenas a ampla defesa é assegurada durante a fase inquisitiva, como por exemplo, o silêncio em oitiva prestada a autoridade policial. A utilização dessas provas, e somente estas, para condenar uma pessoa, iria contra todos os princípios consagrados pela democracia e Constituição Federal de 1988, já que será uma condenação injusta, onde não se deu a oportunidade para o réu se defender de provas que foram obtidas contra ele quando ainda era investigado, ou seja, sem propriamente ter a oportunidade de se defender daquelas, sendo a sentença nesses moldes considerada nula, já que não foi dada elemento essencial do processo – o contraditório-.

Depreende-se esse entendimento após a leitura do *caput* do artigo 155 do mesmo diploma legal[6].

1.3 PROVAS

Segundo Gustavo Badaró[7], prova é

> É apontada como meio pelo qual o juiz chega à verdade, convencendo-se da ocorrência ou inocorrência dos fatos juridicamente relevantes para o julgamento do processo. (...) O juiz tem certeza de um fato quando, de acordo com as provas produzidas, pode racionalmente considerar que uma hipótese fática é a preferível entre as possíveis. Ou seja, em linguagem mais simples, o juiz tem certeza quando as provas o fazem acreditar que o seu conhecimento é verdadeiro.

Prova, em outras palavras, é tudo que o ser humano precisa mostrar, apresentar, ao outro para que comprove, corrobore, fortaleça, tudo aquilo que ele tenha alegado, para

---

[6] Artigo 155: O juiz formará sua convicção pela livre apreciação da prova produzida em contraditório judicial, não podendo fundamentar sua decisão exclusivamente nos elementos informativos colhidos na investigação, ressalvadas as provas cautelares, não repetíveis e antecipadas.

[7] BADARÓ, Gustavo. Processo Penal. São Paulo: Revista dos Tribunais. 2015. p. 377

o possível e mais provável convencimento do outro acerca da veracidade das alegações apresentadas.

No processo penal, ao se tratar da questão de provas, entendemos que é o tema de mais importância perante um processo-crime, já que são a partir destas, ou pela falta delas, que o juiz tomará sua decisão e sentenciar o réu.

Para Gustavo Badaró[8] o tema não somente é o mais importante, mas também o mais difícil:

> eis o ponto mais difícil do processo: proceder à reconstrução histórica dos fatos, de acordo com as regras legais que disciplinam a investigação, a admissão, a produção e a valoração das provas.

São de acordo com as provas, portanto, que o princípio da busca real se baseia. A partir das provas apresentadas, colhidas, produzidas, e o mais importante, sendo submetidas ao contraditório, que o juiz ao tentar se aproximar da verdade real[9] irá condenar ou absolver o agente, não importando a sua opinião, mas sim respeitando o princípio do juiz natural, aplicando a sua imparcialidade, verificando os autos, se está ou não, lastreada de indícios suficientes para tomar a sua decisão, qualquer que seja.

Para Vicente Greco[10], prova é todo o elemento que pode levar o conhecimento de um fato a alguém. Para o autor, a finalidade da prova é o convencimento do juiz, sendo este o destinatário a produção de provas. Para ele, a prova é o meio pelo qual as partes buscarão uma "certeza relativa suficiente na convicção do magistrado"[11].

1.4 MEIOS DE PROVA E MEIOS DE OBTENÇÃO DE PROVA

Segundo explica Gustavo Badaró[12] são considerados meios de prova os instrumentos pelos quais se leva ao processo um elemento de prova apto a relevar ao juiz a verdade de um fato. O Código de Processo Penal elenca, em um rol exemplificativo, a matéria: exame de corpo de delito e perícias em geral (artigos 158 a 184), confissão (artigos 197 a 200), perguntas ao ofendido (artigo 201), testemunhas (artigos 202 a 225),

---

[8] BADARÓ, Gustavo. Processo Penal. São Paulo: Revista dos Tribunais. 2015 p. 377.
[9] A verdade real nunca será alcançada em um processo crime, apesar de todos os meios existentes de investigações modernos que existem, portanto é imprescindível que o juiz alcance um ponto de maior proximidade com a realidade fática para tomar sua decisão.
[10] FILHO GRECO, Vicente. Manual de Processo Penal, 11ª edição. São Paulo: Saraiva. 2015. p.219.
[11] FILHO GRECO, Vicente. Manual de Processo Penal, 11ª edição. São Paulo: Saraiva. 2015. p.220.
[12] BADARÓ, Gustavo. Processo Penal. São Paulo: Revista dos Tribunais. 2015. p. 384.

reconhecimento de pessoas ou coisas (artigos 226 a 228), acareação (artigos 229 e 230), documentos (artigos 231 a 238), indícios (artigo 229) e busca e apreensão (artigo 240 a 250).

Os meios de prova, dessarte, são as ferramentas pela qual o juiz poderá se basear para que se alcance a prova que irá incrementar os autos com documentos que não puderam ser alcançados de maneiras menos gravosas[13].

Difere-se dos meios de obtenção de prova, pois, como explica Gustavo Badaró[14], estes são os instrumentos para a colheita de fontes ou elementos de prova, o qual o Código de Processo Penal disciplina apenas a busca e apreensão (elencada erroneamente nos meios de prova pelo legislador).

Outros meios de prova estão disciplinados em Leis Especiais, como é o caso da Lei 9.296/96, que trata sobre interceptação telefônica. A eficácia dos meios de prova dependem do caráter surpreso, ou seja, sua eficácia se dará com o desconhecimento do investigado-alvo dos meios de prova. A busca e apreensão não surtiria efeitos caso o investigado-alvo soubesse que teria um mandado com essa matéria sobre seus bens-alvos na investigação, assim como a interceptação telefônica não teria resultado se o investigado soubesse que sob sua linha telefônica há um terceiro ouvindo e colhendo tudo que ali estava sendo falado. Importante ressaltar, mais uma vez, que, apesar do desconhecimento do réu, justamente pelo caráter surpreso das medidas, tais provas devem ser levadas ao contraditório, pois o réu deve se defender diante da colheita de tais provas contra si.

Quanto a classificação da prova obtida mediante a quebra do sigilo telemático, devemos traçar uma linha cronológica no tempo e dividir as provas colhidas entre restritiva e ampliativa.

Conforme explica Ricardo Sidi[15]:

> Há duas concepções de prova atípica: a restritiva e a ampliativa. Segundo a primeira, prova atípica é aquela que não nominada em lei, ou seja, que não conta com nenhuma previsão ou menção na legislação. Já na concepcao ampliativa, prova atípica é a que não conta com nenhuma menção ou nominação em lei, mas também é a que é nominada na lei, porém sem previsão de procedimento probatório.

[13] Violentas no sentido da Força Estatal.
[14] BADARÓ, Gustavo. Processo Penal. São Paulo: Revista dos Tribunais. 2015. p. 385.
[15] SIDI, Ricardo. A interceptação das comunicações telemáticas no processo penal. Belo Horizonte: D'Plácido 2016. p. 231.

> Nesse sentido, as interceptações telefónicas e telemáticas no Brasil passaram por três fases: (1) até a promulgação da CF de 1988, eram, sem dúvidas, provas atípicas, fosse pela concepção restritiva, fosse pela ampliativa; (2) após a Constituição e antes da Lei 9.296/96, as interceptações, pela concepção restritiva, tornaram-se provas típicas, porém, pela ampliativa, continuavam a ser atípicas, por falta de procedimento legal; e, por último (3), após a Lei 9.296/96, passaram a ser consideradas provas típicas segundo ambas as concepções.

Seja a medida de busca e apreensão, com fundamento no Código de Processo Penal ou a aplicação da Lei 9.296/96, são medidas cautelares de meios de obtenção de prova, e o fruto, o material colhido, serão tratados como meios de prova.

1.5 PRESSUPOSTOS PARA A REQUISIÇÃO DA QUEBRA DE SIGILO

As exigências para se obter autorização judicial para a interceptação telemática estão cumulativamente disciplinadas na própria Lei 9.296/96. São elas: (i) a existência de indícios razoáveis de da autoria ou participação em infração penal (artigo 2º, I); (ii) que a infração seja apenada com crime de reclusão (artigo 2º, III); (iii) impossibilidade de que a prova seja feita por outros meios disponíveis (artigo 2º,II).

Por ser providencia cautelar, exige-se a presença de *fumus noni iuris*, expresso na possibilidade da autoria e probabilidade de ocorrência da infração penal, e *periculum in mora*, ou seja, no perigo de que a prova se perca, o que está expresso na exigência de que a prova não possa ser feita por outros meios[16].

Portanto, a medida cautelar atípica que é a quebra de sigilo telemática, é medida que deve ser utilizada como última ferramenta para meios de obtenção de provas, sempre respeitando outras medidas, sejam elas as listadas no Código de Processo Penal ou elencadas em leis especiais. Essa rigidez do legislador para permitir o uso da quebra de sigilo telemática foi para proteger os direitos da privacidade e da intimidade do ser humano, é uma intervenção do Estado na vida pessoal do investigado/réu, o que poderá acarretar diversos prejuízos à vida daquele, como por exemplo, o fornecimento de informações pessoais que foram captadas à época da medida em execução.

[16] SIDI, Ricardo. A interceptação das comunicações telemáticas no processo penal. Belo Horizonte: D'Plácido. 2016. p. 232.

Para Gustavo Badaró[17], os indícios de autoria

> não devem ser entendidas meras suspeitas ou simples possibilidade de o investigado ser autor do crime. Por outro lado, não equivale à certeza. A expressão "indícios razoáveis" indica que deve haver um grau de probabilidade (predomínio de elementos convergentes sobre os elementos divergentes, relativos à autoria delitiva).

Conclui-se então que a quebra de sigilo não poderá ser o primeiro ato do processo investigativo, pois exige-se um grau de probabilidade de que o alvo da medida tenha concorrido para a consumação do crime.

1.6 LEGITIMIDADE

Em se tratar da legitimidade para requerer a quebra de sigilo telemático, devemos, primeiramente, dividi-la em 2 espécies, quais serão explicadas em momento posterior, no capítulo 2: (i) "busca e apreensão" dos dados armazenados e (ii) interceptação de comunicação telemática.

Depreende-se de uma interceptação literal da Lei[18] que os dados cadastrais e os registros de acesso podem ser requisitados diretamente pela Polícia Judiciária ou Ministério Público ao particular, sem a necessidade de ordem judicial determinando a entrega de tais informações. Na contramão, os conteúdos humanos, bem como a

---

[17] BADARÓ, Gustavo. Processo Penal. São Paulo: Revista dos Tribunais. 2015. p. 508.

[18] Artigos 10 e 22, ambos da Lei Federal nº 12.965/14 ("Marco Civil da Internet"): 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.

Art. 22. **A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet. – destaques nosso**

interceptação destes (Lei 9.296/96) exige-se prévia ordem judicial autorizando a obtenção dos dados.

O legislador previu a possibilidade do Ministério Público e da Polícia Judiciária requisitarem diretamente aos particulares informações que são menos intrusivas na vida íntima do investigado. Tais informações são menos gravosas em relação a pessoa do que uma comunicação entre e-mails, propriamente falando. Uma dessas exceções, onde não há a necessidade de prévia ordem judicial, está disposta na Lei 9.613/98, com a redação incluída pela Lei 12.683/12, que legisla sobre os crimes de lavagem de dinheiros[19].

Em crimes que versam sobre os crimes de "lavagem" ou ocultação de bens, direitos e valores, portanto, independe de ordem judicial para o requerimento dos dados cadastrais do usuário, quais sejam os que informam "*qualificação pessoal, filiação e endereço*". Essas informações, muitas vezes, não são conferidas pelos responsáveis dos dados, o que o acesso à eles, muitas vezes os tornam inúteis para uma investigação criminal, porém, foi dada a faculdade para a autoridade policial e o Ministério Público requisitarem sem prévia ordem judicial. Muito embora os dados cadastrais e os registros de acesso podem ser alterados pelo próprio usuário[20] para possível ocultação de crime, ou de se esquivar em futura investigação, a regra para a obtenção desses dados dependem, necessariamente, de determinação judicial, dado a sensibilidade que tais informações podem ser para a pessoa.

De outra forma, está previsto no art. 22 que o particular também pode requerer ao juiz a determinação da medida cautelar, mesmo em processo-crime, para o fornecimento de registros de conexão ou de registro de acesso a aplicações da internet. Apesar de não estar explicito o requerimento de particular para os dados cadastrais, nosso entendimento é que o direito de se postular sobre os dados mencionados se estendem ao particular. Os dados cadastrais, muitas vezes, mal são conferidos pelos responsáveis de rede e conexão, razão pela qual o fornecimento desses dados muitas vezes não são conclusivos, e simplesmente expositivos.

---

[19] 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.

[20] Exige-se, para tanto, um grau de conhecimento sobre tecnologia e o desejo de ocultar informações para se esquivar de uma eventual investigação criminal;

Em procedimento ordinário comum, a autoridade policial poderá representar pela quebra de sigilo durante o procedimento inquisitivo. Já o representante do Ministério Público poderá requerer a diligência, seja durante o inquérito, seja ao longo do processo.

Em crimes de ação privada, apesar de não previsto na medida, compartilhamos do entendimento de Gustavo Badaró[21] que o querelante poderá requerer a diligência, afinal, na ação penal privada, ele será o acusador, assim como o Ministério Público é o autor da ação penal pública.

Quanto à aplicação da Lei 9.296/96, que trata sobre as interceptações telefônicas e telemáticas, conforme o art. 1º da Lei, depende de ordem judicial, ou seja, não há a possibilidade de o Ministério Público ou a Autoridade Policial decretarem a medida de ofício. Caso os faça, será considerada prova ilícita.

Quanto ao particular, a lei de interceptação de comunicação é silente. Não há nenhuma restrição, porém nenhuma autorização legitimando o requerimento da vítima. No entanto, nosso entendimento diverge de André Augusto e André Pires Kehdi[22] que defendem ser legítimo a interceptação proposta pela vítima:

> Quanto à vítima, é silente a lei atual. Pela amplitude de crimes a que se aplica (entre eles, por exemplo, o de estupro, que, em regra, é de ação penal privada), não se poderia excluir a legitimidade para propor a interceptação.

À época em que foi escrito o artigo em que se foi retirada a citação anterior, o crime de estupro ainda era de ação penal privada. Não obstante, com introdução cada vez maior da sociedade nos assuntos políticos-sociais, crimes como o de estupro, por exemplo, que não podem ser de ação penal privada, justamente pelo caráter ofensivo que é considerada a conduta do agente e o perigo que ele pode trazer para a sociedade, os crimes apenados com reclusão, quais são tratados pela lei em questão, abrangem os tipos penais que proporcionam um risco maior à vitima e a sociedade, portanto, estão no rol de crimes que o Ministério Público, como fiscal da Lei, não pode desistir da ação e, sempre que possível, investigar em busca da verdade real. Ora, se todas as vítimas tivessem o direito de propor uma interceptação de comunicação, o volume desses

[21] BADARÓ, Gustavo. Processo Penal. São Paulo: Revista dos Tribunais. 2015. p. 511.
[22] MANDES MACHADO, André Augusto e ANDRADE KEHDI, Andre Pires , et al. Sigilo das Comunicações e de dados in Sigilo no Processo Penal. São Paulo, 2008: Revista dos Tribunais. p. 254.

requerimentos seria exponencial, retirando, assim, o caráter da pretensão punitiva estatal e formando uma espécie de direito penal-privado.

1.7 A AUTORIZAÇÃO JUDICIAL PARA A QUEBRA DE SIGILO

É indispensável autorização judicial determinando a quebra do sigilo das comunicações telemáticas ou a interceptação dessas, salvo as exceções já mencionadas e outras que decorrem de lei especiais.

Para fins da quebra do conteúdo já armazenado, está disposto na Lei Federal 12.968/14 ("Marco Civil da Internet"), parágrafo 1º, que este poderá ser disponibilizado apenas mediante ordem judicial. Por outro lado, está disciplinado na Lei 9.296/96, em seu art. 1º que a interceptação dependerá de ordem judicial.

Diante disso, podemos concluir que as provas obtidas mediante ordem de autoridade policial ou do Ministério Público com essa finalidade, são provas ilegítimas e devem, com base no artigo 157 do Código de Processo Penal, ser desentranhadas do processo, sendo inadmissível a utilização dessas para qualquer decisão judicial.

Ademais, uma prova obtida por meio legal, porém, a qual o processo desta depende de uma lei que discute o processo de adequação do meio para a obtenção for inadequado, viola o art. 5º, LVI, da Constituição Federal, dessa maneira, violando um princípio constitucional.

Não obstante, a decisão que decreta esta medida cautelar, deverá ser específica e fundamentada, sendo encaminhada ao particular (i) ofício e a (ii) decisão fundamentada mostrando o prazo da medida, o alvo, os dados que se buscam, e o porquê da medida ser adotada. Não basta apenas apontar o que se quer, mas exige-se a necessidade da "causa" em que se faz a necessidade da quebra de sigilo, não bastando portanto, ao nosso ver, cópia do requerimento da autoridade policial ou Ministério Público e uma decisão simples do juiz decretando a medida "nos termos do requerimento" dos órgãos inquisitivos.

De outro lado, uma decisão "genérica" vai de afronta com a individualização dos alvos da quebra de sigilo. De certa forma, uma quebra de sigilo genérica poderá atingir pessoas que não possuem nexo de causalidade com o crime que ali está sendo investigado,

violando o direito da privacidade e da intimidade[23] de pessoas que podem ser violadas seus direitos apenas pelo uso de determinado aplicativo, programa, etc.

Como pressuposto da quebra de sigilo e sendo esta a última medida que deve ser decretada para meio de obtenção de prova, deverá constar nos autos provas suficientes que demonstrem indícios suficientes de autoria para que seja autorizada as medidas, assunto que é o entendimento dos Tribunais de 2ª instância, como o Tribunal de Justiça de São Paulo[24]:

---

[23] Artigo 5º, inc. X da Constituição Federal

[24] **Mandado de Segurança. Pretendida anulação de decisão judicial. Quebra de sigilo telemático genérico. Violação à privacidade e à individualização do afastamento do sigilo. Região em que se encontra grande fluxo de pessoas. Liminar deferida. Segurança concedida. Decisão anulada.**
1. Trata-se de mandado de segurança , com pedido de liminar, impetrado pelas empresas GOOGLE BRASIL INTERNET LTDA. e GOOGLE LLC, alegando violação ao direito líquido e certo do sigilo das comunicações e privacidade telemática, apontando como autoridade coatora o MM. Juiz de Direito da 3ª Vara Criminal da Comarca de Santa Fé do Sul (Inquérito Policial nº 0001378.90.2018.8.26.0541). Dos autos, consta que o MM. Juízo da 3ª Vara Criminal da Comarca de Santa Fé do Sul determinou, em decisão datada de 1º de agosto de 2018, afastamento de sigilo para que a empresa ora impetrante forneça informações cadastrais dos usuários cujos celulares estavam disponíveis no dia 19/02/2018, entre às 00h00 e às 03h00, em três coordenadas distintas. Sustentam os impetrantes, em síntese, que a determinação de quebra de sigilo telemático é manifestamente inconstitucional e desproporcional, por violar a exigência legal de individualização dos alvos de quebra de sigilo, sendo a ordem genérica e exploratória, solicitando dados de usuários não identificados. Dessa forma, requerem os impetrantes que seja concedida medida liminar para suspensão dos efeitos do ato impugnado e impedimento de eventuais sanções oriundas do descumprimento desse ato. No mérito, pugnam pela anulação da decisão. Oposição ao julgamento virtual manifestado pelo impetrante à fls. 141. Informações recebidas da digna autoridade impetrada à fls. 142/143. Parecer favorável da PGJ à fls. 145/148. É o relatório. 2. É caso de concessão da segurança, anulando a decisão fustigada. Vejamos. 2.1. A quebra de sigilo genérica, sem individualização alguma em relação ao alvo da medida, é vedada pelo ordenamento pátrio, estabelecendo a Constituição da República, em seu art. 5º, inc. XII, a inviolabilidade do "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". Nesse sentido, a Lei 8.771/16, responsável por regular a quebra de sigilo a que faz menção o Marco Civil da Internet, pontua expressivamente a impossibilidade de requisição de pedidos coletivos, genéricos ou inespecíficos, como observado no caso em tela. A decisão proferida pelo juízo de primeiro grau afeta todos os usuários que utilizaram os aplicativos e serviços da impetrante no dia 19/02/2018, entre 00h00 e 03h00, em um raio de 50, 100 e 150 metros das coordenadas geográficas 20°11'18.3"S 50°55'37.7"W, onde ocorreu crime que se busca apurar. Ora, mediante simples consulta digital à coordenada, verifica-se que o referido alcance (50m, 100m e 150m) abrange, dentre outras coisas, um estacionamento, um hotel e uma universidade particular. A quebra de sigilo, portanto, representaria na violação à privacidade de pessoas que guardam nenhuma conexão com os autos, sendo, portanto, manifestamente inconstitucional. Ademais, dispõe o art. 2º, inciso II, da Lei 9.296/96, que não será admitida a interceptação telefônica quando a prova não puder ser feita por outros meios disponíveis. A partir da prova pré-constituída juntada aos autos, não restou clara a impossibilidade de se recorrer a outros meios de prova. 3. Ante o exposto, existente direito líquido e certo das impetrantes, concedo a segurança pleiteada, anulando a decisão fustigada, proferida pelo MM. Juízo da 3ª Vara da Comarca de Santa Fé do Sul, datada de 1º de agosto de 2018. (g.n.)
TJ/SP. Mandado de Segurança 2240432.19.2018.8.26.0000. Relator: Desembargador Otávio de Almeida Toledo. 16ª Câmara de Direito Criminal. DJe: 06/02/2019. Disponível em: <https://esaj.tjsp.jus.br/cposg/search.do;jsessionid=D8ABCAED88A1BBE4CCD8170F8595D506.cposg4?conversationId=&paginaConsulta=1&localPesquisa.cdLocal=-1&cbPesquisa=NUMPROC&tipoNuProcesso=UNIFICADO&numeroDigitoAnoUnificado=2240432-19.2018&foroNumeroUnificado=0000&dePesquisaNuUnificado=2240432-19.2018.8.26.0000&dePesquisa=&uuidCaptcha=>. Acesso em: 10/05/2019.

Daí, extraímos a necessidade e importância de os provedores de rede e conexão avaliarem cada ordem judicial, analisando se esta está de acordo com os parâmetros legais e se não violam os quesitos de “adequação”, “necessidade” e “proporcionalidade em sentido estrito”.

1.8 O PROCESSAMENTO DA ORDEM PELO PARTICULAR

Os provedores de internet e aplicação são contratualmente responsáveis pela preservação da inviolabilidade do conteúdo das correspondências, sendo assim, têm o direito de acesso ao conteúdo das decisões judiciais que terminem o afastamento do sigilo que proteja o conteúdo das comunicações realizadas pelos seus usuários ou pelos diversos dados que possas surgir ao acessar a rede.

Ao receber uma ordem, o particular deve verificar se todos os requisitos estão devidamente preenchidos de acordo com a Lei a qual se submete, seja o caso de interceptação de conteúdo ou de busca e apreensão dos dados armazenados. Por conta disso, a simples determinação judicial, comunicada via ofício ou de outras formas, é insuficiente para permitir que os referidos provedores concluam pela legalidade ou ilegalidade da ordem, impossibilitando o imediato cumprimento da medida.

Nesse sentido, o particular que fornece informações de maneira negligente, sem ter feito a prévia conferência dos parâmetros legais, poderá responder criminalmente e civilmente, já que é de responsabilidade objetiva àquele que viola direito de outrem, independentemente de ser auferida o grau de culpa.

Por outro lado, quando se verificado que a ordem é manifestamente ilegal, por qualquer razão, o particular tem o dever de não fornecer as informações requisitadas. Tal dever impõe ao particular o direito de, perante o Requerente, seja este em fase inquisitória ou no bojo de uma ação penal, explicar o motivo do não municiamento ao Requerente.

A Constituição Federal assegura, em seu art. 5º, inc. XXXVII, que nenhuma lesão ou ameaça a direito será excluída da apreciação do Poder Judiciário. Se os provedores forem impedidos de terem o acesso à decisão, estes não poderão saber se os requisitos legais foram preenchidos, e não terão como levantar a questão em juízo ou até cumprir ordem manifestamente genérica.

1.9 DAS HIPÓTESES QUE PODEM SURGIR APÓS A COMUNICAÇÃO DA QUEBRA DE SIGILO

Após levantar a questão da ilegalidade da ordem, o particular cumpriu seu papel no processo. Ora, ele foi requisitado e logo após justificou a impossibilidade de cumprir a ordem. Não há mais o que fazer. Dessa maneira, duas das possibilidades que vislumbramos a partir deste momento poderá ser a omissão ou concordância do Requerente.

Após o protocolo do particular, a autoridade poderá simplesmente continuar com o processo, sem tomar uma decisão quanto à petição que alega o Provedor a impossibilidade jurídica de cumpri-la. Dessa maneira, presume-se que as informações ora requisitadas não são mais necessárias ou que, pelo menos, diante de uma nova manifestação do juiz, exime o particular de tomar quaisquer outras providências.

Por conseguinte, acarreta à mesma hipótese uma decisão em que o Requerente concorde, ou não impugna, a justificação do particular, sendo que este cumpriu seu papel e aquele compreendeu e concordou com a situação em concreto.

Outra possibilidade é o responsável pelo provedor incorrer sob o crime de desobediência, previsto no art. 330 do Código Penal, tipificando a conduta de particular em desobedecer ordem legal de funcionário público no exercício da função. Dessa maneira, poderá incorrer o particular que desobedecer ordem legal da medida cautelar em crime de desobediência.

A situação em concreto deverá ser analisada, pois o particular pode entender que a ordem é ilegal e deixar de cumpri-la, sendo assim, juntando documentos no curso do inquérito que apura sua desobediência, e provando que sua conduta foi atípica.

Como destaque, a última hipótese que trazemos é a de eventual imposição ao particular de cumprir a ordem, sob pena de multa e responder criminalmente pelo já mencionado art. 330 do Código Penal.

O particular não pode cumprir ordem mediante coação da autoridade Requerente. A imposição de multa, ameaçar aquele de responder criminalmente ou até alegar uma suposta ilegitimidade do particular ao levantar a ilegalidade da ordem são questões de extrema relevância no Processo Penal em um Estado Democrático de Direito.

Dessa maneira, cabe ao particular o dever de impugnar tais decisões com tons de ameaça, pois em um processo crime, que é a medida mais drástica do Estado para punir alguém, não pode ser exercida de forma autoritária, eis que as leis impõe limites para o manejo de qualquer situação durante o processo.

Não obstante, aquele que ceder à ameaça poderá responder na esfera cível, criminal e administrativa, conforme está previsto no art. 12, I e II da Lei Federal nº 12.965/14[25]:

Posto isso, para combater tal medida de imposição do cumprimento de ordem manifestamente ilegal, resta ao particular o manejo de Mandado de Segurança, no qual deverá demonstrar (i) a impossibilidade de cumprir ordem manifestamente ilegal, (ii) a não tipificação do crime de desobediência, (iii) requerer ao Tribunal de eximi-lo de pagamento de multa e (iv) declarar a ordem que acarretou no Mandado de Segurança ilegal, sendo assim, desobrigando-a de cumpri-la, entre outros pedidos a depender do caso concreto.

Em decisões recentes, os tribunais superiores[26] estão reconhecendo e declarado a legitimidade do dever de agir das provedoras de rede e conexão, mesmo não estando inseridas no polo passivo, nem ativo, de inquéritos e ações penais:

---

[25] 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;

[26] MANDADO DE SEGURANÇA. IMPETRAÇÃO POR TERCEIRO. **LEGITIMIDADE**. QUEBRA DE SIGILO TELEMÁTICO. INEXISTÊNCIA DE INDÍCIOS DE PRÁTICA CRIMINOSA. SEGURANÇA CONCEDIDA. 1. Mandado de segurança impetrado por Google Brasil Internet Ltda. impugnando decisão pela qual o Juízo, em medida cautelar penal, determinou à impetrante a quebra do sigilo de dados telemáticos em relação a sete vídeos divulgados por terceiros no YouTube, que é uma plataforma de compartilhamento público de vídeos mantida pela impetrante. 2. Impetrante sustenta, em suma, que o Juízo determinou a identificação dos usuários que inseriram os vídeos no YouTube, daqueles que visualizaram os vídeos e dos que fizeram o download dos vídeos; que, quanto às pessoas que teriam inserido ou divulgado os vídeos no YouTube, verificou-se que os vídeos foram inseridos no território do Chile, o que inviabiliza o cumprimento da ordem;; que em relação às pessoas que visualizaram o vídeo, inexiste qualquer traço de conduta ilícita na mera visualização de vídeo inserido no YouTube, que é uma plataforma pública de compartilhamento de vídeos; que no tocante às pessoas que teriam efetuado o download dos vídeos, a determinação é de impossível cumprimento porque os vídeos inseridos no YouTube não são passíveis de download; que a decisão padece de ausência de fundamentação válida para justificar a quebra do sigilo de dados de um número indeterminado de pessoas; que a determinação impugnada implicou a quebra do sigilo de dados de súditos estrangeiros. Requer a concessão da ordem para desobrigá-la de cumprir a determinação impugnada. Liminar indeferida. Parecer da PRR1 pela extinção do processo, sem resolução do mérito, diante da perda superveniente do interesse processual. 3. **"A impetração de segurança por terceiro,**

2. MODALIDADE DE DADOS

2.1 DADOS CADASTRAIS

Tais dados são aqueles que, supostamente, são os menos intrusivos na privacidade e intimidade do usuário. São meramente qualificativos, como nome, e-mail, endereço, telefone, etc. Estes são a exigência mínima para que você possa acessar um site, efetuar compras online, etc. Na realidade, as empresas não fazem uma busca para saber se tais informações que o usuário preencheu são verdadeiros ou não, ou seja, estes dados muitas vezes podem ser inverídicos perante o alvo da medida cautelar.

De fato, para as empresas que exigem o pré-cadastramento em seus serviços com essas informações, não pretendem, a priori, conhecer melhor o usuário, mas sim dar o primeiro passo para de fato “invadir” o mundo virtual daquele, de maneira que no início dessa relação usuário-empresa, não há grandes violações quanto à intimidade e vontade do usuário. As empresas passam a mandar e-mails de publicidade e propaganda, e conforme os cliques dos que recebem as ofertas, passam-se a entregar os gostos pessoais àquelas, e a partir daí então, que os dados passam a ser mais sensíveis.

Portanto, por ora, estamos numa relação inicial, onde as informações aqui prestadas podem ser verídicas ou não, sem que haja uma possibilidade técnica para os

---

contra ato judicial, não se condiciona a interposição de recurso." (STJ, Súmula 202, CORTE ESPECIAL, julgado em 17/12/1997, DJ 02/02/1998, p. 181.) (A) Considerando que a impetrante não participa da relação processual da medida cautelar, tem ela direito, nos termos da Súmula 202 do STJ, de interpor o presente mandado de segurança, independentemente da interposição de recurso. (B) Por outro lado, e, tendo em vista que o Juízo não revogou a determinação impugnada, persiste o interesse processual da impetrante na resolução do mérito do pedido. Consequente conhecimento do presente mandamus. 4. A concessão de mandamus que impugna ato judicial demanda do impetrante a demonstração, de forma clara e convincente, mediante prova documental idônea e inequívoca, de que o ato judicial "se revest[e] de teratologia, ilegalidade ou abuso flagrante". (STF, RMS 28082 AgR; TSE, AgRg em MS nº 169597.) Dessa forma, somente em situações excepcionais, nas quais estejam demonstrados, de forma clara e convincente, e mediante prova documental idônea e inequívoca, a teratologia, a ilegalidade ou o abuso de poder, na decisão judicial, será cabível a concessão da segurança. 5. Quebra de sigilo de dados telemáticos. Indícios de autoria e ou de participação em crime doloso punido com reclusão. Lei 9.296, de 1996, Art. 2º, I. Ausência de demonstração razoável. (A) No que respeita às pessoas que visualizaram os vídeos a ordem é manifestamente ilegal, porquanto inexiste conduta criminosa na mera visualização de vídeo de qualquer natureza. (B) No tocante às pessoas que fizeram o download dos vídeos, a ordem é de impossível cumprimento, porquanto os vídeos hospedados no YouTube não são passíveis de download. CPC, Art. 374, I, e Art. 375. (C) Quanto às pessoas que inseriram ou divulgaram os vídeos no YouTube, o Juízo deixou de demonstrar que essa conduta, por si só, é criminosa, como, por exemplo, no caso de divulgação de "vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente". Lei 8.069, de 1990, Art. 241-A. 6. Segurança concedida. (g.n.)TRF-1. Mandado de Segurança 00332150620174010000. Relator: Desembargador Federal Mário César Ribeiro. Segunda Seção. DOU: 28/09/2018. Disponível em: <https://processual.trf1.jus.br/consultaProcessual/processo.php >. Acesso em: 10/05/2019.

particulares confirmarem tais informações, senão vejamos, por exemplo, a enorme rede de usuários que existem na plataforma de e-mails da Google (*Gmail)* ou da Microsoft (*Hotmail)*. Qualquer pessoa pode possuir mais de um e-mail em qualquer uma provedora, prestando informações diversas das que foram prestadas na criação da conta anterior, portanto, é impossível, muitas vezes, para os provedores fazerem as conferências de tais dados, tornando-os muitas vezes inúteis para o recolhimento destas durante uma investigação criminal.

Diante de tal grau superficial a respeito da intimidade e privacidade do usuário, o art. 10, §3º do Marco Civil da Internet dispõe que as autoridades administrativas podem requisitar esses dados, sem prévia ordem judicial. Essas autoridades não estão descritas na lei 12.965/14, mas sim previstas em outras duas leis de formas expressas. São elas a lei nº 9.613/18 (Lavagem de Dinheiro) e a Lei nº 12.850/13 (Organização Criminosa). O art. 17-B, quanto o art. 15 das respectivas leis, dispõem que a autoridade policial e o Ministério Público poderão acessar, independentemente de ordem judicial, os dados cadastrais do investigado, nas formas que a Lei dispuser.

2.2 DADOS DE TRÁFEGO

Entende-se como dados de tráfego as informações que são geradas a partir do envio de mensagens, e-mails, acesso a sites e afins, no mundo online. Como bem define Ricardo Sidi[27], trata-se, por exemplo, da identificação do remetente e do destinatário, à hora do envio da mensagem, à localização dos interlocutores através das ERBs utilizadas durante a chamada, à quantidade de *bytes* transmitidos, ao volume do áudio (se se tratar de comunicação de áudio), à duração do diálogo, aos IPs utilizados pelos interlocutores e ao custo da comunicação.

Para limitar o escopo dessas informações, iremos gozar de termo usado no cotidiano, sendo que todos as informações (dados) que são gerados e mencionados supra, podem ser englobados em *logs de acesso*, com exceção ao endereço IP.

Os *logs de acesso***,** portanto, são os dados inerentes ao uso de determinadas ferramentas da internet que transmitem dados de tráfego, sendo estes gerados e

[27] SIDI, Ricardo. A interceptação das comunicações telemáticas no processo penal. Belo Horizonte: D'Plácido 2016. p. 109.

resguardados pelos particulares, sem o conhecimento do usuário, já que ele foi um vestígio deixado para trás apenas pelo fato do usuário ter realizado algum acesso na rede.

Por outro lado, endereço IP (*Internet Protocol)* é um conjunto de números que identifica o seu dispositivo ao acessar a uma rede de internet. É a identificação do seu computador ou dispositivo móvel, que é gerada a partir do momento que ele se conecta com a internet e utiliza dos dados de tráfego. Assim, a partir desse conjunto de números que é gerado, é possível descobrir a fonte daquele uso de dados alvo da investigação, por exemplo.

O legislador conceitua o significado do endereço IP, no inciso III do art. 5º: "o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais". Quando um terminal de computador se conecta a internet, no caso de conexão mediante IP dinâmico, o endereço IP é atribuído pela interface do computador, ou automaticamente, usando o DHCP (*Dynamic Host Configuration Protocol).* Esse endereço IP jamais é fornecido pelo usuário de internet ao provedor, mas sim, é automaticamente atribuído ao se conectar a internet. Por outro lado, é vedada ao provedor coletar, utilizar ou tratar esse endereço IP que foi gerado.

De forma equivocada o Marco Civil disciplina ambas as espécies de dados como "registros de conexão", em seu art. 5º, inciso VI, e que são tratadas no art. 13 da citada Lei. Tal artigo dispõe sobre os métodos que devem ser aplicados à guarda, fornecimento e competência para requisição dos dados.

Destrinchando o art. 13 e seus respectivos parágrafos do Marco Civil da Internet, observamos que o endereço IP e os *logs de acesso* devem ser mantidos em sigilo pelo provedor de rede, pelo prazo de até um ano (da data de cada acesso), sendo possível ainda que, mediante requisição policial ou ministerial, que as provedoras mantém esses dados por mais tempo, até que sobrevenha autorização judicial para obtê-las, em até 60 dias após o pedido.

Sendo assim, não incorre sob pena de multa ou crime, o provedor que alegar não possuir mais os dados que foram requisitados mediante ordem judicial ou até pela representação do Ministério Público e autoridade policial, após o período de 1 ano.

O citado artigo está em consonância com a Resolução 614, de 28 de maio de 2013, expedida pela Anatel[28].

Como bem destaca Dámasio de Jesus[29], as autoridades policias, administrativas ou o Ministério Público podem requerer às provedoras que estas preservem os dados que se pretendem buscar por mais tempo, até que sobrevenha ordem judicial para o fornecimento destas. Desta maneira, as provedoras deverão preservas os dados até 60 dias, do requerimento das aludidas autoridades, até decisão judicial determinando o fornecimento destes dados.

Portanto, são dados resguardados pelo sigilo, que também deverão ser fornecidos observados os requisitos da Lei, com a devida fundamentação do juiz e selecionando, especificamente, os alvos da medida.

2.3 COMUNICAÇÃO HUMANA

Importante salientar antes de mais nada, que a invasão à comunicação humana é a maneira mais intrusiva, ou a que mais viola o direito à intimidade e privacidade do investigado. Não por menos, a Constituição Federal de 1988 tutela a proteção do sigilo das correspondências e das comunicações telegráficas, em seu artigo 5º, inciso XII.

A comunicação se dá pela ação de transmitir uma mensagem a outrem. Para existir uma comunicação, portanto, é evidente que precisamos de 2 ou mais interlocutores. Alguém precisa transmitir alguma informação e alguém precisa receber essa informação. Não há comunicação quando temos apenas 1 interlocutor e isso será de suma importância

---

[28] Art. 53. A Prestadora deve manter os dados cadastrais e os Registros de Conexão de seus Assinantes pelo prazo mínimo de um ano.

[29] O art. 13 prevê, ainda, em seu § 2o, a possibilidade de autoridades policiais, administrativas ou mesmo do Mi- nistério Público em requererem cautelarmente que os registros sejam guardados por mais tempo, em uma situa- ção específica. Logicamente, este requerimento deverá ser feito no prazo de até um ano desde o acontecimento, pois após este período, mesmo com o requerimento, o provedor poderá ter apagado os registros. Após o requerimento mencionado, a autoridade po- licial, administrativa ou o Ministério Público terá que requerer judicialmente o acesso a tais dados, no prazo de 60 (sessenta) dias. Importante destacar que os provedores não devem fornecer os registros mediante requerimento de autoridades policiais, administrativas ou do Ministério Público, mas aguardar a ordem ou o mandado judicial. A autoridade terá 60 (sessenta) dias para ingressar com o pedido judicial dos dados, dos quais requereu ao pro- vedor a custódia por mais tempo. Caso a ordem judicial seja indeferida, o requerimento de preservação de dados perderá a eficácia. JESUS, Damásio de. Marco Civil da Internet. São Paulo: Saraiva. 2014. p. 56.

para a aplicabilidade da Lei 9.296/96, a qual não poderá interceptar informações que não se enquadrem no termo “comunicação”.

Os e-mails são uma forma de correspondência, protegidos pelo art. 5º, caput, inc. XII, na parte que garante o sigilo da correspondência. O fato de se tratar de uma correspondência eletrônica não altera a natureza da liberdade pública envolvida. Uma vez que se trata de liberdade de manifestação do pensamento de forma reservada e à distância, o fato de se tratar de uma correspondência eletrônica poderá ter repercussão na definição do meio de obtenção de prova cabível, quando da necessidade de obtenção do conteúdo de e-mails relevantes para um processo-crime.

2.4 DADOS DIVERSOS DE COMUNICAÇÃO

Neste tópico, iremos expor dados que não se submetem a nenhuma categoria anteriormente já dita e apontar a lacuna que existe na Lei para a hipótese de interceptação destas.

Diferentemente do que previu o legislador, há ferramentas, aplicativos, programas, que não se enquadram em (i) dados cadastrais, (ii) endereço de IP, (iii) logs de acesso ou (iv) comunicação humana. De fato, esses dados inominados podem ser equiparados à um tipo de conteúdo já armazenado, sujeitos à busca e apreensão.

Esses dados podem ser desde documentos salvos em nuvens (*clouds*), quanto às fotos salvas nos dispositivos do usuário ou até os contatos da agenda de cada usuário. Esses dados podem ser obtidos mediante ordem judicial, com base no Marco Civil da Internet, fazendo analogia quanto aos dados ali descritos na lei, embora não estão sujeitos à Lei 9.296/96, como passaremos a expor adiante.

Portanto, os dados diversos de comunicação são todos aqueles que não estão no bojo das classificações que o legislador previu no Marco Civil da Internet.

3. DOS MEIOS DE OBTENÇÃO DE PROVA

3.1 BUSCA E APREENSÃO

Para Gustavo Badaró[30], a medida de busca e apreensão, é um meio de obtenção de provas, em que a busca ou eventual apreensão de coisa ou pessoa não basta, sendo necessária, após a conservação das provas obtidas, a produção da prova correspondente realizada diretamente pela fonte.

Como ensina Bastos Pitombo[31], a busca é uma medida instrumental, a qual visa encontra pessoas ou coisas, já a apreensão é uma medida cautelar probatória, pois se destina à garantia de prova. Logo, podemos concluir que a primeira é ato meio e a segunda, ato fim. Para apreender algo, é necessária a sua busca, logo, a apreensão, que pode ser frutífera ou não, depende da busca, do interesse de obter alguma coisa que eventualmente poderá ser juntada como fonte de prova.

Evidente que a busca e apreensão, como medida cautelar, afronta certos princípios, como os da intimidade, vida privada e os da dignidade da pessoa humana.

De antemão, frisa-se o certo apontamento de Aury Lopes Jr[32]: "Mas os direitos fundamentais não são absolutos e podem ser restringidos. A busca e apreensão trabalham nessa exceção da proteção constitucional. São, por isso, medidas excepcionais".

Assim, a medida de busca e apreensão afronta o direito a privacidade e intimidade da pessoa humana, que possuem tutela ampla de proteção, conforme explica Cleunice Pitombo[33]:

> A intimidade e a vida privada não são asseguradas, tão-só, com a impossibilidade de violação de domicílio, da correspondência e com a proibição das interceptações telefônicas. O âmbito da tutela é maior e se ramifica em vários instantes, no curso da persecução penal. Acham-se, ainda, protegidos, no sistema jurídico, da seguinte forma: (a) proteção contra danos morais por ataques à dignidade da pessoa; (b) tipos penais de injúria, calúnia e difamação; (c) inviolabilidade de domicílio; (d) a contravenção penal de perturbação de tranquilidade.

Portanto, nota-se que apesar de ser uma violação lícita do poder Estatal, há limites que devem ser respeitados quanto à dignidade da pessoa humana.

---

[30] BADARÓ, Gustavo. Processo Penal. São Paulo: Revista dos Tribunais. 2015. p. 491.
[31] JÚNIOR, Aury Lopes. Direito Processual Penal. São Paulo: Saraiva. 2014.. p. 507.
[32] JÚNIOR, Aury Lopes. Direito Processual Penal. São Paulo: Saraiva. 2014.. p. 506.
[33] PITOMBO, Cleunice Bastos. Da Busca e Da Apreensão No Processo Penal. São Paulo: Revista dos Tribunais. 2005. p.81.

Tal medida está prevista nos artigos 240 a 250 do Código de Processo Penal e poderá ser utilizada para a obtenção dos 4 tipos de dados que foram mencionados supra.

Mesmo antes da publicação do Marco Civil da Internet, em casos de grande repercussão nacional, o Superior Tribunal de Justiça[34] entendia que era possível a apreensão dos dados já armazenados pelos provedores de Rede e Conexão.

Isso ocorre diante do fato que o poder Estatal legitima a violação ao direito fundamental do sujeito, que não pode se esquivar dos fatos que lhe são imputados ao armazenar eventuais provas que podem acarretar em uma condenação, em forma de documentos virtuais.

Após a referida Lei entrar em vigor, restou claro a diferença entre os dados já armazenados - esses pacíficos de busca e apreensão- e a incidência da Lei 9.296/96, que trata sobre a interceptação de comunicação.

É importante salientar, portanto, a diferença de tais dados, já que os armazenados, que estamos tratando neste tópico, são aqueles já previamente gerados nos servidores de conexão e rede, e que ali devem permanecer, segundo a Lei, por até um ano.

---

[34]**PROCESSUAL PENAL. OPERAÇÃO "LAVA-JATO". MANDADO DE BUSCA E APREENSÃO. APREENSÃO DE APARELHOS DE TELEFONE CELULAR. LEI 9296/96. OFENSA AO ART. 5o, XII, DA CONSTITUIÇÃO FEDERAL. INOCORRÊNCIA. DECISÃO FUNDAMENTADA QUE NÃO SE SUBORDINA AOS DITAMES DA LEI 9296/96. ACESSO AO CONTEÚDO DE MENSAGENS ARQUIVADAS NO APARELHO. POSSIBILIDADE. LICITUDE DA PROVA. RECURSO DESPROVIDO.**

I - A obtenção do conteúdo de conversas e mensagens armazenadas em aparelho de telefone celular ou smartphones não se subordina aos ditames da Lei 9296/96. II - **O acesso ao conteúdo armazenado** em telefone celular ou smartphone, quando determinada judicialmente a busca e apreensão destes aparelhos, não ofende o art. 5o, inciso XII, da Constituição da República, porquanto o sigilo a que se refere o aludido preceito constitucional é em relação à interceptação telefônica ou telemática propriamente dita, ou seja, é da comunicação de dados**, e não dos dados em si mesmos.** III - Não há nulidade quando a decisão que determina a busca e apreensão está suficientemente fundamentada, como ocorre na espécie. IV - Na pressuposição da ordem de apreensão de aparelho celular ou smartphone está o acesso aos **dados que neles estejam armazenados, sob pena de a busca e apreensão resultar em medida írrita, dado que o aparelho desprovido de conteúdo simplesmente não ostenta virtualidade de ser utilizado como prova criminal**. V - Hipótese em que, demais disso, a decisão judicial expressamente determinou o acesso aos dados armazenados nos aparelhos eventualmente apreendidos, robustecendo o alvitre quanto à licitude da prova. Recurso desprovido. (destacamos) Superior Tribunal de Justiça. RHC nº 75800. Relator: Felix Fischer. Quinta Turma. DJE: 26/09/2016. Disponível em: < https://ww2.stj.jus.br/processo/pesquisa/>. Acesso em: 10/05/2019.

Os Tribunais demonstram esse entendimento ao pacificar a questão, mostrando que não há a inocorrência de prova ilícita quando assim obtidos esses dados, sejam eles de comunicação ou diversos de comunicação[35].

Embora isso, ainda há no que se falar em prova ilícita quando não preenchidos os requisitos da Lei, como por exemplo, ausência de autorização judicial. Nesse caso, com a devida proteção constitucional, em seu art. 5º, LVI, que esclarecer ser inadmissíveis as provas ilícitas, cumulado com o art. 157 do Código de Processo Criminal, estas deverão ser desentranhadas do processo, sendo consideradas nula, senão vejamos a seguinte decisão do Superior Tribunal de Justiça[36]:

---

[35] **DIREITO PROCESSUAL PENAL. MANDADO DE SEGURANÇA. INQUÉRITO POLICIAL. INVESTIGAÇÃO. DELITOS DE ASSOCIAÇÃO CRIMINOSA E CARTEL. MANDADOS DE BUSCA E APREENSÃO. FORMA DE CUMPRIMENTO. EXTRAÇÃO DE DADOS DE SERVIDOR DA EMPRESA. CAIXAS DE E-MAILS. EXTENSÃO SUBJETIVA DA ORDEM CONSTRITIVA. PREVISÃO. AUSÊNCIA DE ILEGALIDADE**. 1. **Não se deve confundir quebra do sigilo das comunicações de dados com os próprios dados, armazenados em equipamentos de informática, que podem vir a ter seu sigilo quebrado quando apreendidos nos equipamentos em decorrência de cumprimento de mandados de busca e apreensão**. Precedentes. 2. Ausente ilegalidade na conduta da Autoridade Policial que, ao constatar que os dados de e-mail corporativo ficavam armazenados em um servidor central localizado em outro estado da Federação, além de haver impossibilidade técnica do recebimento dos dados na mesma data em que cumpridos os mandados na sede da empresa, colheu compromisso da mesma, na pessoa de um funcionário, para que algumas contas de e-mails fossem entregues à Superintendência da Polícia Federal no prazo assinalado - tendo tal apreensão expressamente sido autorizada no mandado de busca e apreensão expedido. 3. **O sigilo de informações e dados constitucionalmente protegidos não se transmuda em direito absoluto, devendo ser ponderado diante do resguardo do interesse público, verificado no caso de indícios de cometimento de delitos** e, ainda, mais acentuado no caso em apreço, onde se constata possível prática de cartel, com aptidão para lesar inúmeros consumidores . 4. Ainda que os impetrantes não estivessem formalmente sendo investigados no Inquérito Policial, certo é que a empresa, na qual possuem cargos estratégicos, estava. Sendo assim, os dados dos e-mails funcionais podiam ser objeto de extração por parte da autoridade policial acaso se entendesse haver neles elementos de convicção relacionados aos fatos objeto do inquérito policial, tal como constou do mandado de busca e apreensão expedido. 5. Segurança denegada. (g.n.) TJ/DF. Mandado de Segurança 0007637-74.2016.8.07.0000. Relator: Desembargador César Laboissiere Loyola. Câmara Criminal. DJe: 24/06//2016. Disponível em: <https://cache-internet.tjdft.jus.br/cgi-bin/tjcgi1?NXTPGM=plhtml02&TitCabec=2%AA+Inst%E2ncia+%3E+Consulta+Processual&SELECAO=1&CHAVE=0007637-74.2016.8.07.0000&COMMAND=ok&ORIGEM=INTER>. Acesso em: 10/05/2019.

[36] **PROCESSUAL PENAL. RECURSO EM HABEAS CORPUS. TRÁFICO DE DROGAS. INTERCEPTAÇÃO TELEFÔNICA. ACESSO DE MENSAGENS DE TEXTO VIA WHATSAPP. AUSÊNCIA DE AUTORIZAÇÃO JUDICIAL. GARANTIAS CONSTITUCIONAIS. ART. 5º, X E XII, DA CF. ART. 7º DA LEI N. 12.965/2014. NULIDADE. OCORRÊNCIA. CONSTRANGIMENTO ILEGAL CONFIGURADO. RECURSO EM HABEAS CORPUS PROVIDO.** 1. **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**. 2. A Lei n. 12.965/2014, conhecida como Marco Civil da Internet, em seu art. 7º, assegura aos usuários os direitos para o uso da internet no Brasil, entre eles, o da inviolabilidade da intimidade e da vida privada, do sigilo do fluxo de suas comunicações pela internet, bem como de suas comunicações privadas armazenadas. 3**. A quebra do sigilo do correio eletrônico somente pode ser decretada, elidindo a proteção ao direito, diante dos requisitos próprios de cautelaridade que a justifiquem idoneamente, desaguando em um quadro de imprescindibilidade da providência.** (HC 315.220/RS, Rel. Ministra MARIA THEREZA DE

É necessário, portanto, que os objetos alvos da medida da quebra de sigilo telemático sejam pretéritos à emissão da ordem. Para a efetiva busca e apreensão dos dados, estes, devem já estar armazenados nos sistemas dos provedores de rede e conexão. Como requisito obrigatório da medida, é necessário que haja fundada suspeita perante o acusado

No mais, a medida deverá sempre ser sigilosa, e indicando as pessoas que poderão ter acesso ao conteúdo obtido, já que se tratam de informações da intimidade e privacidade do sujeito, ou seja, que afrontam diretamente princípios constitucionais. Aponta corretamente Aury Lopes Jr[37] que caso não fossem acobertados pelo sigilo, a medida poderia ser prejudicial para a própria investigação: "imprescindível então que a medida e seu resultado sejam mantidos em sigilo, sem permitir-se o bizarro espetáculo midiático, tão prejudicial para a imagem e intimidade do imputado, como também para a própria investigação".

Vale frisar que apesar de sigilosa, qualquer medida cautelar no curso de inquéritos e ações penais, após encerrada e colhidas as provas, juntando-as nos autos, deverão ser então disponíveis a defesa do réu, sob pena de restrição ao contraditório e ampla defesa. Vale a nota de Maurício Zanoide[38] sobre o tema:

> Idealmente, o investigado deverá ter acesso aos autos no instante em que sua esfera de direitos passe a sofrer restrições em decorrência da investigação perpetrada. Contudo, para a execução de certas medidas persecutórias, seria inviável permitir o seu acesso aos autos ou a parte deles enquanto aquelas não findarem. Nessas hipóteses, enquanto o ato sigiloso, determinado segundo os pressupostos e requisitos de proporcionalidade, esteja sendo executado, não poderá o investigado ter acesso à, ou saber de parte da, investigação. Porém, encerrada a razão que justificava o sigilo ínsito à medida requerida, caso não haja outro fato impeditivo, da mesma natureza, ainda em curso (outras

---

ASSIS MOURA, SEXTA TURMA, julgado em 15/09/2015, DJe 09/10/2015). 4. Com o avanço tecnológico, o aparelho celular deixou de ser apenas um instrumento de comunicação interpessoal. **Hoje, é possível ter acesso a diversas funções, entre elas, a verificação de mensagens escritas ou audível, de correspondência eletrônica, e de outros aplicativos que possibilitam a comunicação por meio de troca de dados de forma similar à telefonia convencional.** 5. **Por se encontrar em situação similar às conversas mantidas por e-mail, cujo acesso é exigido prévia ordem judicial, a obtenção de conversas mantidas pelo programa whatsapp, sem a devida autorização judicial, revela-se ilegal.** 6. Recurso em habeas corpus provido para declarar nula as provas obtidas no celular do recorrente sem autorização judicial, determinando que seja desentranhado, envelopado, lacrado e entregue ao denunciado do material decorrente da medida. (g.n.) STJ. Recurso em Habeas Corpus 75055-DF 2016/0219888-7. Relator: Ministro Ribeiro Dantas. Quinta Turma. DJe: 27/03/2017. Disponível em: <https://ww2.stj.jus.br/processo/pesquisa/>. Acesso em: 10/05/2019.

[37] JÚNIOR, Aury Lopes. Direito Processual Penal. São Paulo: Saraiva. 2014. p. 506.

[38] ZANOIDE DE MORAES, Maurício, et al. Publicidade e Proporcionalidade in Sigilo no Processo Penal. São Paulo, 2008: Revista dos Tribunais. p. 47

> diligências intrinsicamente sigilosas), o sujeito que sofreu a medida deve ter acesso a todo o conteúdo da investigação.

Diferentemente o que ocorre com a Lei 9.296/96, que trata sobre as interceptações telefônicas, para a busca e apreensão dos dados armazenados, não há no que se falar em requisitos sob a natureza dos dados, sendo todos estes aptos à violação (legítima) estatal[39].

3.2 INTERCEPTAÇÃO DA COMUNICAÇÀO TELEMÁTICA

O conceito de telecomunicação no ordenamento jurídico brasileiro está disposto no artigo 60, §1º da Lei nº 9.472/90[40], que é "a transmissão, emissão ou recepção, por fio, radioeletricidade, meios ópticos ou qualquer outro processo eletromagnético, de símbolos, caracteres, sinais, escritos, imagens, sons ou informações de qualquer natureza". Como já mencionado, exige-se para a celebração da comunicação humana, 2 sujeitos, no mínimo. Um irá transmitir ou emitir a informação que deseja passar a outrem – no caso, o 2º sujeito- quem irá receber aquela mensagem.

Interceptar, segundo o Dicionário da Língua Portuguesa Houaiss é: "verbo transitivo direto, é interromper o curso de algo; impossibilitar o funcionamento (ligação, comunicação etc); captar (mensagem, comunicação de outrem) sem que perceba isso quem se comunica". Para a sua aplicação no caso deste estudo, é preciso, como bem aponta Vicente Greco[41] ao afirmar que "a interceptação é a violação feita por terceiro em face de dois interlocutores, não se aplicando, pois, à conduta unilateral de um deles.", sendo assim, considera-se a interceptação telemática como um meio de obtenção de provas.

A inviolabilidade do sigilo das comunicações está prevista no artigo 5º, inc. XII da Constituição Federal de 1988. Presume-se, portanto, que a comunicação pode ser realizada pelas pessoas que vivem no Brasil, um Estado Democrático de Direito, e que a privacidade e a intimidade dos sujeitos que estão se comunicando, devem ser respeitadas, sob o sigilo garantido pela Carta Magna.

---

[39] Vale ressaltar que as senhas dos usuários que eventualmente podem ser salvas em diferentes plataformas não se encaixam no rol de dados armazenados aptos a serem recolhidos. Isso, no nosso entendimento, afetaria um nível de intervenção estratosférica na vida do acusado, podendo levar o Estado a uma quantidade de informação muito maior do que se fez jus à emissão da medida.

[40] Lei Nº 9.472, de 16 de julho de 1997. Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº 8, de 1995.

[41] GRECO, Vicente. Interceptação Telefônica: considerações sobre a lei n. 9.296/96. São Paulo: Saraiva. 2015, 3ª Edição. p. 65.

Embora amparados pela Constituição Federal, o direito a intimidade e privacidade podem ser violados, para que o poder Estatal não fique enfraquecido quanto à conduta da população. Vale a nota de Guilherme de Moraes[42] :

> Pelo fio do exposto, o sigilo representa uma projeção do direito à intimidade, cuja quebra é condicionada à decisão fundamentada de autoridade judicial competente, sem embargo da possibilidade de requisição de Comissão Parlamentar de Inquérito,29 porquanto "a quebra de sigilo bancário, fiscal ou telefônico, atividade que se reveste de extrema gravidade jurídica e cuja prática pressupõe, necessariamente, a competência do órgão judiciário ou legislativo que a determina, só deve ser decretada, e sempre em caráter de excepcionalidade, quando existentes fundados elementos de suspeita que se apoiem em indícios idôneos, reveladores de possível autoria de prática delituosa por parte daquele que sofre a investigação penal, competência realizada pelo Estado. A relevância da garantia do sigilo, que traduz uma das projeções realizadoras do direito à intimidade, impõe, por isso mesmo, cautela e prudência na determinação da ruptura da esfera de intimidade que o ordenamento jurídico, em norma de salvaguarda, pretendeu subordinar à cláusula de reserva constitucional", com fundamento no art. 3º, incs. I e II, da Lei nº 9.296/96, art. 1º, § 4º, da Lei Complementar nº 105/01 e art. 198, § 1º, do CTN.30

O ser humano é um ser sociável, possuindo laços com mais de uma pessoa. Desses laços, observamos o grau de intimidade de cada um. Ora, ninguém contaria um segredo íntimo a uma pessoa desconhecida, ou, mesmo sendo conhecida, não possua um grau elevado de afetividade. Posto isso, a comunicação é intrínseca à intimidade e privacidade do sujeito, como conclui Ricardo Sidi[43]:

> Tal direito, à inviolabilidade do sigilo das comunicações, permite ao particular excluir do conhecimento de terceiros indesejados, aí incluído, é claro, o próprio Estado, o conteúdo de suas comunicações e os dados ligados a comunicações concretas."

No entanto, para que a realização da interceptação seja de fato frutífera para as investigações, não se admite que qualquer dos interlocutores saibam da existência da medida. Caso isso ocorresse, não seria uma interceptação, e sim, possuiria outros termos em que a Lei nº 9.296/96 não previu, conforme explica Eduardo Santos[44]:

> Outro aspecto importante é que na interceptação está ínsita a presença de um terceiro que não seja um dos interlocutores e que, ademais, não lhes seja de conhecimento. Veremos adiante que quando um dos participantes da comunicação produz a gravação ou tem ciência dela, descaracteriza-se a figura da interceptação (...).

---

[42] PENÃ DE MORAES, Guilherme. Curso de Direito Constitucional, 11ª edição. São Paulo: Atlas, 2019. p.195.

[43] SIDI, Ricardo. A interceptação das comunicações telemáticas no processo penal. Belo Horizonte: D'Plácido. 2016 p. 215.

[44] CABETTE, Eduardo Santos. Interceptação Telefônica, 3ª edição. São Paulo: Saraiva. 2015. p. 31.

A Lei 9.296/96 trata sobre o tema de interceptação do fluxo de comunicação telefônica e telemática. Como já mencionados, os pressupostos para decretar o ato são (i) a existência de indícios razoáveis da autoria ou participação em infração penal, (ii) que esta infração seja cominada com pena de reclusão e a impossibilidade de que a prova seja feita por outros meios disponíveis, sendo então de última *ratio* a sua possibilidade.

Vale aqui frisar que o art. 2º da referida Lei recebe críticas de inúmeros autores, como Vicente Greco Filho[45], por ela possuir uma redação negativa, ou seja, enumera as possibilidades em que não são possíveis a decretação da interceptação (de qualquer modalidade). Sendo assim, as hipóteses em que caibam a interceptação poderão ir muito além do que o legislador realmente imaginou (ou não), já que ele lista as que não são passíveis da aplicabilidade da Lei, deixando um leque de hipóteses muito maior do que as taxativamente previstas nela.

A partir do recebimento da ordem judicial, o provedor de rede e conexão que deve cumprir a ordem, irá captar todas as mensagens de comunicação que envolve o alvo da medida[46], e após o prazo estipulado na ordem, que não poderá ultrapassar 15 dias – prazo este previsto no art. 5º da Lei- fornecerá o que foi recolhido para quem lhe competiria.

O prazo máximo para a medida é de 15 dias, renováveis por mais 15 (art. 5º). Embora há espaço para a renovação da medida, que deveria ser considerada sempre em última hipótese, a 6ª Turma do STJ[47] consolidou o entendimento de que as decisões que

---

[45] GRECO FILHO, Vicente. Manual de Processo Penal. São Paulo: Saraiva. 2012

[46] Frisa-se, aqui, que a ordem judicial deve especificar o serviço de comunicação que se pretende interceptar. No mundo digital dos dias de hoje, não há como uma decisão aplicar a Lei 9.296/96 em sistemas telegráficos com a ausência do produto que se vislumbra. Uma empresa, como a Google por exemplo, possui muitos variados meios que os usuários possam se comunicar. Uma quebra de sigilo genérica, por outro lado, seria ineficaz e não produz efeitos jurídicos, já que a empresa não deve proceder de maneira que ela entende, violando o sigilo do usuário e fornecendo todos os dados do investigado de todos os meios que goza de comunicação com outras pessoas que nada importaria àquela investigação.

[47] HABEAS CORPUS. SUCEDÂNEO DO RECURSO ORDINÁRIO. INADMISSIBILIDADE. INTERCEPTAÇÃO TELEFÔNICA. INQUÉRITO CIVIL PÚBLICO. IDENTIFICAÇÃO DE INDÍCIOS RAZOÁVEIS DE PRÁTICA DELITIVA. INAUGURAÇÃO DE VEIO INVESTIGATIVO-CRIMINAL. PLEITO DA CONSTRIÇÃO DIRECIONADO AO JUÍZO CRIMINAL. ILEGALIDADE. AUSÊNCIA. FUNDAMENTAÇÃO EXISTENTE E SUFICIENTE. QUEBRA DO SIGILO DAS COMUNICAÇÕES. **PRAZO SUPERIOR A 15 DIAS. POSSIBILIDADE. PRORROGAÇÃO AUTOMÁTICA. INOBSERVÂNCIA DO DEVER DE MOTIVAR AS DECISÕES JUDICIAIS. CONSTRANGIMENTO ILEGAL CARACTERIZADO. DESENTRANHAMENTO DAS PROVAS ILÍCITAS E DAQUELAS DELAS DERIVADAS.** [...] 6. A despeito de contrariar a literalidade desse dispositivo legal, a limitação do prazo para a realização de interceptações telefônicas não constitui óbice ao deferimento da medida excepcional por período superior a 15 dias, desde que haja circunstanciada justificação. Precedentes. 7. A prorrogação da quebra de sigilo, não obstante a jurisprudência admitir tantas quantas necessárias, pode ocorrer, mas nunca automaticamente, dependendo sempre de decisão judicial fundamentada, com específica indicação da indispensabilidade da continuidade das diligências.8. No caso, o magistrado, ao autorizar interceptações do fluxo de comunicações em sistema de telemática originadas e

prorrogaram as interceptações tragam fundamentação idônea e adequada, não sendo suficiente um mero "despacho" que reiteraria os termos da primeira.

O procedimento inicia-se no dia útil subsequente ao recebimento da ordem, pelo particular. Aqui, diferentemente do tópico anterior, estamos tratando de eventuais dados futuros. A medida pode ser frutífera ou não, é um direito futuro incerto, já que o alvo, mesmo com o desconhecimento da medida em execução, poderá não utilizar dos meios alvos da medida para se comunicar, ou usa-los e não ser vantajoso em nada para aquela investigação.

A aplicação da Lei 9.296/96, pelo todo já exposto, deverá ser medida excepcionalíssima, justificável e justificada, analisada o caso concreto. Dada a excepcionalidade da medida, devem-se observar outras medidas cautelares que devem anteceder esta, como meios de prova, por exemplo provas testemunhais. Não sendo estas possíveis, e sendo adequada uma medida de obtenção de prova, deve se preferir a busca e apreensão do tópico supra, ao invés da aplicação da interceptação telemática.

Assim explica Gustavo Badaró[48], quanto a decisão determinando a quebra de sigilo telemática, tanto qualquer outra decisão judicial, deverá ser fundamenta, demonstrando todos os aspectos que envolvem a legitimação para a decretação da medida cautelar, sendo assim, preenchendo os requisitos que são impostos pela Lei:

> A impossibilidade deve ser justificada com a demonstração de que a investigação é inviável por outros meios, por exemplo, a busca e apreensão, o reconhecimento pessoal, as provas testemunhais, a obtenção dos registros das ligações telefônicas, etc. Por óbvio, não basta repetir os termos da lei e afirmar que a investigação não poderia ser realizada por outros meios. É necessário indicar, concretamente, por que a reconstrução dos fatos será impossível sem a interceptação telefônica.

De ponto de vista da teoria geral da prova, todo e qualquer meio de prova, bem como os meios de obtenção de provas, devem obedecer os requisitos lógicos de

---

recebidas de determinados números de telefone pelo prazo de 15 dias, prorrogáveis automaticamente por mais 15 dias, e por 30 dias seguidos, não apresentou motivação concreta, caracterizando abusividade, a justificar a declaração de ilicitude de tais provas e daquelas delas derivadas. (destaque nosso) TJ/DF. Mandado de Segurança 0007637-74.2016.8.07.0000. Relator: Desembargador César Laboissiere Loyola. Câmara Criminal. DJe: 24/06//2016. Disponível em: <https://cache-internet.tjdft.jus.br/cgi-bin/tjcgi1?NXTPGM=plhtml02&TitCabec=2%AA+Inst%E2ncia+%3E+Consulta+Processual&SELECAO=1&CHAVE=0007637-74.2016.8.07.0000&COMMAND=ok&ORIGEM=INTER>. Acesso em: 10/05/2019..

[48] BADARÓ, Gustavo. Processo Penal. São Paulo: Revista dos Tribunais. 2015. p. 508.

pertinência e de relevância probatória, que serão delimitados a partir do fato concreto objeto da imputação.

No que tange à determinação da interceptação telemática, urge salientar que as comunicações que porventura possam estar armazenadas não poderão ser fornecidas, salvo se na mesma ordem há expressa e fundamentada decisão contrária. Ora, se o juiz ao determinar o monitoramento da comunicação do investigado por 15 dias, por exemplo, a busca e apreensão já deveria ter sido emanada anteriormente, o que impede de o particular de fornecer conteúdo diferente daquele que foi expressamente citado pelo juiz. Ou seja, caso as autoridades inquisitivas achem as provas obtidas mediante uma interceptação não vantajosas, deverão estes representar por uma nova quebra de sigilo, seja ela mediante busca e apreensão ou uma nova aplicação da Lei 9.296/96.

A Lei prevê a possibilidade do juiz decretar a medida de ofício.

Em nosso entendimento, não é constitucional o juiz decretar a medida de ofício, pois estaria violando o princípio do juiz imparcial, sendo o fruto dessa eventual medida, prova ilegal. O princípio do juiz imparcial é uma garantia essencial para um processo penal mais justo. Há correntes doutrinárias que defendem que o juiz poderia decretar de ofício apenas durante a ação penal, não sendo possível durante o curso do inquérito. De outro lado, a corrente minoritária que apoiamos, defendida por Gomes e Cervini[49] entende que a decisão da medida de ofício, torna o juiz em um "juiz inquisidor", o que afeta a sua imparcialidade perante o processo. Ora, o juiz não deve se satisfazer pelas provas contidas nos autos, mas não deve ele agir para que se corrobore as provas contidas nos autos. Caso haja insuficiência de provas e o Ministério Público não requerer demais diligências (ou a autoridade policial), deve-se aplicar o princípio do *in dubio pro reo*, absolvendo-o ou rejeitando eventual denúncia com insuficiência de autoria delitiva.

3.3 INTERCEPTAÇÃO DE DADOS DIVERSOS DE COMUNICAÇÃO

A lei 9.296/96 regulamenta o inciso XII do art. 5º da Constituição Federal, disciplinando a exceção da inviolabilidade das comunicações[50] para meio de obtenção de prova em investigação criminal e em instrução penal.

[49] BADARÓ, Gustavo Processo Penal. São Paulo: Revista dos Tribunais. 2015. p. 511.
[50] Para este tópico, não importa dizer comunicação telemática, já que esses dados não são "comunicação" propriamente ditos.

Com efeito, a lei apenas será aplicada quando existir uma comunicação, ou seja, há 1 agente que transmite uma informação a outra.

Os dados diversos de comunicação[51] são informações geradas pelo próprio usuário mediante o uso de programas, aplicativos, acessos, ferramentas da internet. Esses dados são armazenados pelo próprio usuário de maneira intencional ou não. O uso de ferramentas que permite o usuário de rede guardas documentos em nuvem – as famosas *clouds* –, bem como o armazenamento de fotos em aplicativos, senhas pessoais para acessos em sites, são exemplos de dados que o sujeito pode armazenar da maneira que bem entender em seu sistema, o que ficará salvo também nos sistemas dos provedores de rede e conexão.

De maneira não intencional, temos como exemplo a localização do usuário que poderá ser rastreada pelo uso do GPS, se estiver ativo no aparelho eletrônico, bem como o histórico de pesquisa de um navegador específico[52].

Dessa maneira, a busca e apreensão dos dados já gerados, ou seja, que estão devidamente armazenados são passíveis de busca e apreensão, nos termos dos artigos 240 a 250 do Código de Processo Penal.

De outra forma, esses dados não se encaixam na modalidade "comunicação". O sujeito que deseja salvar os contatos, fotos, senhas, não o faz com intuito de passar para outrem, e sim de armazenar e deixa-las em um lugar seguro para si mesma. Dessa maneira, não há no que se falar em comunicação dos dados que não foram (ou serão) gerados para o uso próprio. O interesse do sujeito não é compartilhar essa informação com outra pessoa, senão utilizaria de ferramentas próprias de se comunicar, como encaminhando um e-mail, ou mediante uma mensagem via Whats App, com esses contatos, fotos, senhas ou outras inúmeras possibilidades.

Desta maneira, o alvo da medida de interceptação que deseja ter o conhecimento dessas informações que poderão ser geradas após a data de

---

[51] Vide tópico 2.4

[52] Colocamos esse exemplo como "não intencional", pois ao realizar pesquisas o usuário não pretende que aquelas pesquisas fiquem salvas. Ele busca o que quer encontrar, pouco importando o histórico de buscas, pois o que importa é o que ele há de encontrar no navegador, não o que ele pesquisou no passado.

emissão da ordem, deve especificar o produto de comunicação e não de maneira diversa, determinando que o provedor o faça por intermédio de produtos que interessam apenas o sujeito.

Portanto, há uma lacuna na lei sobre a possibilidade de interceptação desses dados, já que não são comunicação, ou seja, não são passíveis da aplicação da medida cautelar da lei 9.296/96.

Decisões judiciais que determinem a provedora de conexão e rede a procederem a interceptação desses dados são ilegais, pois não há previsão legal que diz ser possível o monitoramento desses dados.

De maneira equivocada, decisões de tribunais superiores[53] não conseguem visualizar que esses dados não são sujeitos à aplicabilidade da lei 9.296/96.

---

[53] 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. 5. As Turmas que compõem a 3ª Seção desta Corte têm entendido que "a imposição de astreintes à empresa responsável pelo cumprimento de decisão de quebra de sigilo, determinada em inquérito, estabelece entre ela e o juízo criminal uma relação jurídica de direito processual civil", cujas normas são aplicáveis subsidiariamente no Processo Penal, por força do disposto no art. 3º do CPP. Nesse sentido, "a solução do impasse gerado pela renitência da empresa controladora passa pela imposição de medida coercitiva pecuniária pelo atraso no cumprimento da ordem judicial, a teor dos arts. 461, § 5.º, 461-A, do Código de Processo Civil, c.c. o art. 3.º do Código de Processo Penal" (RMS 44.892/SP, Rel. Ministro RIBEIRO DANTAS, Quinta Turma, julgado em 05/04/2016, DJe 15/04/2016). 6. A legalidade da imposição de astreintes a terceiros descumpridores de decisão judicial encontra amparo também na teoria dos poderes implícitos, segundo a qual, uma vez estabelecidas expressamente as competências e atribuições de um órgão estatal, desde que observados os princípios da proporcionalidade e razoabilidade, ele está implicitamente autorizado a utilizar os meios necessários para poder exercer essas competências. Nessa toada, incumbe ao magistrado autorizar a quebra de sigilo de dados telemáticos, pode ele se valer dos meios necessários e adequados para fazer cumprir sua decisão, tanto mais quando a medida coercitiva imposta (astreintes) está prevista em lei. 7. Muito embora no Direito Civil a exigibilidade da multa diária por

Nota-se que além da comunicação realizada pelo usuário, havia ordem que determinava a interceptação de senhas e de fotos com seus respectivos metadados. A decisão supra não está correta, pois há diferença entre as espécies de dados, conforme demonstrado ao longo deste trabalho.

Não obstante, a lei 9.296/96 não alcança os dados que não integram a comunicação do sujeito. Não há no que se falar em descumprimento de medida que obrigue a provedora em interceptar aqueles que não fazem parte da comunicação humana. Estes são passíveis, portanto, de busca e apreensão, com fundamento nos artigos 240 a 250 do Código de Processo Penal, e não sob a ótica da Lei 9.296/96.

No mais, vale a lição de Gustavo Badaró[54], que bem distingue, com, cada vez mais, o crescimento exponencial de surgimentos de novas ferramentas, aplicativos, programas, métodos que os usuários utilizam a internet, de novos surgimentos de dados e a necessidade que o legislador, os órgãos inquisitivos e as provedoras de rede e de conexão precisam encaixar os tipos de dados resultantes naqueles conforme a Lei o diz claramente:

> todavia, embora irretocável em suas premissas quanto, de um lado, à instantaneidade da comunicação e à possibilidade de interceptação e, de outro, à perenidade do instrumento da comunicação e apreensão de tal elemento, é de considerar que a própria evolução da tecnologia alterou as características da comunicação de dados. Partia-se da premissa de que a comunicação dos dados era não instantânea e, portanto, permitia a apreensão. Diz o autor: como vimos,

descumprimento de decisão judicial esteja condicionada ao reconhecimento da existência do direito material vindicado na demanda (REsp n.º 1.006.473/PR, Rel. Ministro LUIS FELIPE SALOMÃO, Rel. p/ Acórdão Ministro MARCO BUZZI, QUARTA TURMA, julgado em 08/05/2012, DJe 19/06/2012), sob pena de enriquecimento sem causa do autor (destinatário do valor da multa), o mesmo raciocínio não se aplica ao Direito Penal, em que o destinatário do valor das astreintes é o Estado, titular da pretensão punitiva, e em que não existe motivo para condicionar-se a exigibilidade da multa à condenação do réu. 8. Ao determinar o bloqueio dos valores o juiz não age como o titular da execução fiscal, dando início a ela, mas apenas dá efetividade à medida coercitiva anteriormente imposta e não cumprida, tomando providência de natureza cautelar. E isso se justifica na medida em que a mera imposição da multa, seu valor e decurso do tempo parecem não ter afetado a disposição da empresa recorrente em cumprir a ordem judicial. De se lembrar que o art. 139, IV, do CPC/2015, autoriza o juiz a "determinar todas as medidas indutivas, coercitivas, mandamentais ou sub-rogatórias necessárias para assegurar o cumprimento de ordem judicial, inclusive nas ações que tenham por objeto prestação pecuniária". 9. A renitência da empresa em cumprir a determinação judicial por mais de um ano justifica a incidência da multa coercitiva prevista no art. 461, § 5º, do CPC no valor de R$ 50.000,00 (cinquenta mil reais), que não se revela excessivo, diante do elevado poder econômico da empresa, até porque valor idêntico foi adotado pelo STJ na QO-Inq n. 784/DF e no RMS 44.892/SP. 10. Recurso ordinário em mandado de segurança a que se nega provimento. STJ. Recurso em Mandado de Segurança 55.109/PR 2017/0215256-6. Relator: Ministro Reynaldo Soares da Fonseca. Quinta Turma. DJe: 17/11/2017. Disponível em: < https://ww2.stj.jus.br/processo/pesquisa/>. Acesso em: 10/05/2019.

[54] BADARÓ, Gustavo. Processo Penal. São Paulo: Revista dos Tribunais. 2015.. p. 505.

> o inciso XII (proteção da comunicação de dados) impede o acesso à própria ação comunicativa, mas não aos dados comunicados1". Hoje, contudo, há diversas formas de comunicação em sistemas de telemática, cujos dados não permanecem armazenados em sistemas de computadores. Em outras palavras, há comunicação instantânea de dados, que consequentemente não admite apreensão dos dados comunicados, e comunicações de dados seguidas do armazenamento dos elementos comunicados, em que não se faz necessária a interceptação da comunicação, bastando a apreensão dos dados, como forma menos gravosa e menos excessiva de restrição da privacidade.

Por fim, vale destacar que, além dos dados diversos de comunicação tratados neste tópico, a lei nº 9.296/96 autorizando apenas a medida em casos de comunicação, é ilegal uma decisão judicial determinando seja interceptada os dados de tráfego, expostos no tópico 2.2. Esses dados, por não terem o objeto "comunicação" intrínsecos a eles, não são passíveis de monitoramento, e sim, de busca e apreensão, como aponta Luiz Flávio Gomes e Silvio Maciel[55]:

> É uma lei que cuidou das "comunicações" que estão acontecendo (atuais, presentes). Não alcança, portanto, os registros telefônicos que são "dados" relacionados com comunicações telefónicas passadas, pretéritas. Mas negar a incidência da Lei 9.296/96 no que concerne à quebra dos dados telefónicos não significa que eles não possam ser devassados. De outro lado, não se pode refutar a ideia de que a Lei 9.296/96, no que concerne aos requisitos, abrangência, limites, venha servir de parâmetro para o juiz (por causa do principio da proporcionalidade) na hora de se determinar a quebra do sigilo desses dados. Mas não foi intenção do legislador disciplinar a quebra do sigilo telefónico na Lei em estudo. E não cabe analogia em matéria de direitos fundamentais, que estão regidos pelo princípio da legalidade estrita.

[55] GOMES, Luiz Flávio; MACIEL, Silvio. Interceptação telefônica e das comunicações de dados e telemáticas: comentários a Lei 9.296/96 – 4ª ed. São Paulo: Editora Thompson Reuters Brasil, 2018. P.61.

Conclusão

O presente trabalho tratou de estudar os principais aspectos da medida cautelar de Quebra de Sigilo Telemático no processo penal brasileiro. Em um primeiro momento, vislumbramos que quaisquer que sejam os direitos fundamentais do ser humano, podem ser violados pela força – legítima – estatal. Com isso, para o curso de um inquérito policial ou ação penal, pode ser decretada a medida cautelar em questão, quando forem preenchidos os requisitos legais das respectivas lei de meios de obtenção de prova. Nesse sentido, deve, em qualquer hipótese, os provedores de rede e conexão realizarem um procedimento de análise da ordem judicial. Na hipótese da decisão judicial (ou um ofício extrajudicial) determinando a quebra de sigilo de dados for manifestamente ilegal, concluímos que os mesmos são legítimos para realizarem a impugnação da ordem, seja por uma petição simples endereçada a autoridade competente, ou via o Mandado de Segurança.

A aplicabilidade das leis existentes para a decretação da quebra de sigilo telemático, dependerão sempre das modalidades dos dados que se almeja. Para isso, no capítulo 2, expusemos os tipos de dados existentes hoje no mundo da informática. São eles (i) dados cadastrais; (ii) dados de tráfego; (iii) comunicação humana; (iv) e dados diversos de comunicação. O primeiro refere-se aos dados pessoais do usuário, os quais são obtidos pelos provedores em um primeiro momento de acesso perante o produto ali que deseja-se usar, como nome, endereço, telefone, etc. Dados de tráfego são os registros que são gerados pelo acesso, pelo uso da rede pelo usuário. Normalmente, esses dados são gerados de forma automática, ou seja, o usuário, muitas vezes, não sabe da existência desses dados, pois eles não ficam registrados para o próprio usuário, mas sim para os provedores. Comunicação humana são os dados gerados a partir de uma conversa, troca de mensagens, informações entre um locutor e um interlocutor. Necessita-se, portanto, para que seja enquadrado aqui, um produto-meio que seja propriamente de comunicação, ou seja, sua finalidade seja passar para outrem algum tipo de informação, seja ela por foto, documento, mensagens, etc. Por fim, os dados diversos de comunicação são aqueles que não podem ser inseridos em nenhuma categoria anterior. São aqueles dados frutos de produtos fornecidos que, principalmente, não são de comunicação, ou seja, são dados pessoais, gerados a partir da vontade do usuário, porém, que não necessariamente foram gerados para ser compartilhado (leia-se “comunicado”) a outrem.

As modalidades que tratamos na presente monografia foram as Leis Federais nº 9.296/96 (Lei de Interceptção Telefônica e Telemática) e a medida de busca e apreensão, previsto no Código de Processo Penal. A primeira visa obter as comunicações (ainda não realizadas) posteriores à emissão da ordem. Isso será realizado com a introdução de um 3º (no nosso caso, os provedores de rede e conexão) que irão captar, sem o conhecimento do alvo da medida, toda a comunicação realizada durante o período máximo de 15 (quinze) dias. A aplicabilidade da referida lei trata-se apenas das comunicações telemáticas, portanto, todos os outros 3 (três) tipos de dados que listamos supra, não são passíveis de interceptação, pois estes não são dados gerados a partir de uma comunicação humana.

Quanto à busca e apreensão, esta sim, acoberta todos os tipos de dados armazenados. Aqui, não importa, após a decisão judicial conforme os requisitos de lei, os tipos de dados que se visa obter, sejam eles apenas dados cadastrais ou dados diversos de comunicação. A finalidade de medida é buscar algo materialmente possível, o que é alcançável, uma prova que apenas com uma decisão judicial poderá ser buscada, e consequentemente, apreendida. Não podemos então confundir os dados existentes e as medidas que podem ser utilizadas para alcançar os mesmos. Um, trata-se dos dados já existentes, armazenados. O outro sobre as comunicações futuras, importando apenas a espécie "comunicação", não podendo ser atingida por quaisquer outros dados que divergem de comunicação.

Para um processo penal mais justo, respeitando os direitos fundamentais do ser humano, não se pode cogitar em violações estatais de forma exorbitante, apesar de serem legítimas. Por conta disso, às medidas cautelares no processo penal devem ter tidas com atenção por todas as partes, para garantir o mais nobre acesso à justiça pelo acusado. Dessa maneira, com a facilidade de se obter informações cada vez mais específicas sobre qualquer usuário de internet, as quebras de sigilo devem ser decretadas quando observados os requisitos das leis, não podendo estas serem decretadas diante qualquer hipótese, violando os direitos fundamentais de forma ilegal, acarretando enormes prejuízos à vida de qualquer pessoa.

Referencias Bibliográficas

1. BADARÓ, Gustavo. Processo Penal. São Paulo: Revista dos Tribunais. 2015.

2. CABETTE, Eduardo Santos. Interceptação Telefônica, 3ª edição. São Paulo: Saraiva. 2015.

3. FILHO GRECO, Vicente. Manual de Processo Penal, 11ª edição. São Paulo: Saraiva. 2015.

4. GOMES, Luiz Flávio; MACIEL, Silvio. Interceptação telefônica e das comunicações de dados e telemáticas: comentários a Lei 9.296/96 – 4ª ed. São Paulo: Editora Thompson Reuters Brasil, 2018.

5. GRECO, Vicente. Interceptação Telefônica: considerações sobre a lei n. 9.296/96. São Paulo: Saraiva. 2015, 3ª Edição.

6. JÚNIOR, Aury Lopes. Direito Processual Penal. São Paulo: Saraiva. 2014.

7. MANDES MACHADO, André Augusto e ANDRADE KEHDI, Andre Pires , et al. Sigilo das Comunicações e de dados in Sigilo no Processo Penal. São Paulo, Revista dos Tribunais. 2008.

8. PENÃ DE MORAES, Guilherme. Curso de Direito Constitucional, 11ª edição. São Paulo: Atlas, 2019.

9. PITOMBO, Cleunice Bastos. Da Busca e Da Apreensão No Processo Penal. São Paulo: Revista dos Tribunais. 2005.

10. SIDI, Ricardo. A interceptação das comunicações telemáticas no processo penal. Belo Horizonte: D'Plácido. 2016.

11. TOURINHO FILHO, Fernando da Costa. Processo Penal, volume 1. São Paulo: Saraiva. 2010.

12. ZANOIDE DE MORAES, Maurício, et al. Publicidade e Proporcionalidade in Sigilo no Processo Penal. São Paulo, Revista dos Tribunais. 2008.

TERMO DE AUTENTICIDADE DO TRABALHO DE CONCLUSÃO DE CURSO

Eu, Mohamad Hassan Fares

Aluno(a), regularmente matriculado(a), no Curso de Direito, na disciplina do TCC da 10ª etapa, matrícula nº 41434927 , Período 10 , Turma S ,

tendo realizado o TCC com o título: Quebra de Sigilo Telemático

sob a orientação do(a) professor(a): Marco Aurélio Florêncio Filho

declaro para os devidos fins que tenho pleno conhecimento das regras metodológicas para confecção do Trabalho de Conclusão de Curso (TCC), informando que o realizei sem plágio de obras literárias ou a utilização de qualquer meio irregular.

Declaro ainda que, estou ciente que caso sejam detectadas irregularidades referentes às citações das fontes e/ou desrespeito às normas técnicas próprias relativas aos direitos autorais de obras utilizadas na confecção do trabalho, serão aplicáveis as sanções legais de natureza civil, penal e administrativa, além da reprovação automática, impedindo a conclusão do curso.

São Paulo, 24 de maio de 2019.

Assinatura do discente