ASPECTOS CONSTITUCIONAIS E PENAIS DA INTERCEPTAÇÃO TELEMÁTICA: sua força probante

Umbertino Antônio de Carvalho Neto[1]
Patrícia Barcelos N. de Mattos Rocha[2]

RESUMO

Os meios informatizados, especialmente a rede mundial de computadores, muitas vezes são utilizados para o cometimento de crimes que, pelas características peculiares, são de difícil investigação. O presente estudo tem por finalidade a análise constitucional e penal da prova obtida pela interceptação de dados telemáticos, demonstrando a forma como ela é produzida e utilizada no inquérito policial e na fase processual. Na ausência de uma norma específica, várias situações que permeiam a matéria ficam obscuras, dentre elas a possibilidade ou não da medida cautelar se constituir como prova idônea no processo, mas, sobretudo, o que mais se indaga é como tornar viável a regulamentação do mundo virtual. Quanto à primeira questão, é majoritário o entendimento de ser perfeitamente aceitável a interceptação telemática como instrumento probatório, desde que amparada pelo manto constitucional e legal. Em relação à segunda, não há consenso entre os usuários e a doutrina, visto que a normatização, para os primeiros, seria mitigar a liberdade no ambiente virtual, contrariando a própria essência deste, mas, para os doutrinadores – com algumas divergências – e especialmente o Poder Público, é necessário e urgente, pois os cybercrimes crescem vertiginosamente, pedindo pronto enfrentamento por parte do Estado. Trata-se de uma pesquisa de natureza básica; exploratória, quanto aos objetivos; qualitativa, em relação à abordagem; e bibliográfica, quanto aos procedimentos metodológicos.

PALAVRAS-CHAVE: Sigilo das Comunicações. Interceptação Telemática. Prova.

INTRODUÇÃO

Por muito tempo, o ordenamento jurídico brasileiro andou às escuras com relação à possibilidade ou não de submeter os dados e as comunicações telefônicas à medida cautelar da interceptação, pois na redação do inciso XII, do artigo 5º, da Constituição Federal de 1988, exigia-se a formulação de Lei que estabelecesse seus parâmetros.

[1]Mestre em Segurança Pública-UVV. Especialista em Políticas Públicas de Gênero e Raça-UFES, Especialista em Direito Médico-EMESCAM. <carvalho_neto156@yahoo.com.br>
[2] Mestre em Direito. Especialista em Direito Público. Coordenadora do Curso de Direito Rede Doctum Campus Guarapari/ES. <patricia.nunes@doctum.edu.br>

Inúmeros processos e investigações se iniciaram com base na interceptação telefônica, mesmo com a inércia do legislativo, que visualizava tudo sem se manifestar quanto à edição de uma Lei específica. E essa passividade gerou prejuízos ao Poder Punitivo do Estado, visto que o Supremo Tribunal Federal, exercendo a função de guardiã dos direitos constitucionais, anulava os processos que chagavam à sua apreciação, com base na inexistência de lei que regulamentasse os procedimentos da medida excepcional em tela.

Ademais, o desgaste temporal e financeiro era latente, pois se utilizava da máquina pública quase que com a certeza de que, ao final da ação, tudo seria anulado pela falta de provas inidôneas – argumento predominantemente utilizado pelos Ministros dos Tribunais Superiores – aumentando com isso, também, a sensação de impunidade.

Diante de tal situação, mesmo que tardiamente, o Congresso Nacional editou a norma que veio regulamentar o art. 5° no seu inciso XII, parte final, da CRFB. Trata-se da Lei 9.296, de 24 de julho de 1996, conhecida como a Lei das Interceptações, pois, além de normatizar a interceptação de comunicações telefônicas, também regula a do fluxo de comunicações em sistemas de informática e telemática.

O presente trabalho objetiva, estabelecer as peculiaridades e trazer a discussão sobre a parte extensiva da Lei das Interceptações, quer dizer, as possibilidades e as controvérsias da violação do sigilo dos dados telemáticos e/ou informáticos, bem como a sua utilização como prova no processo penal.

Qualquer sistema jurídico que preze pela concretização de suas normas – da forma mais eficiente possível – carrega consigo a disposição de sempre evoluir conforme a sociedade, até mesmo para que não venha a se tornar um ordenamento inócuo, incapaz de atender à demanda e aos anseios da coletividade.

O que se vislumbra entre o Direito e a Tecnologia é a cooperação de ambos, ou seja, deve-se encontrar um equilíbrio entre a frenética evolução da ciência tecnológica e a segurança trazida pela ciência jurídica, pois esta deve compreender que a sociedade não ficou restrita aos papéis do passado, e aquela deve assimilar que sem regras e limites não há evolução que não vire caos.

É nesse sentido que caminha esta pesquisa, isto é, até que ponto o sistema jurídico brasileiro se abre para o avanço da informática, da computação e, especialmente, da rede mundial de computadores, por onde milhões de pessoas se

comunicam diariamente e, por conseqüência, onde o fluxo de dados telemáticos é imensurável?

Com a evolução da informática e da internet o meio virtual passou a ser um grande instrumento nas relações humanas, sejam elas entre particulares ou entre organismos públicos, desde a simples utilização para contatos sociais, até a realização de atividades mais complexas como, por exemplo, transações financeiras, prestação de serviços, o comércio eletrônico, dentre infinitas outras possibilidades.

Nesse rumo, deve-se entender as peculiaridades das investigações criminais quando se deparam com delitos que, por muitas vezes, podem deixar vestígios imperceptíveis, que, para serem desvendados, demandam paciência e conhecimento técnico apurado dos órgãos investigativos. Além disso, a aceitação desse rastro deixado e gerado de forma eletrônica como prova capaz de incriminar o provável cibercriminoso, quando adquirido através da medida excepcional de interceptação é questão ainda controversa que será devidamente exposta.

Outro ponto importante é a necessidade ou não de regulamentação da internet[i], sendo sopesados os argumentos favoráveis e os desfavoráveis.

Assim, além de apresentar de forma despretensiosa, no sentido de não esgotar o assunto, as características das comunicações de dados telemáticos, objetiva-se entender os aspectos penais e processuais que envolvem a prova produzida a partir da medida excepcional de violação ao sigilo constitucionalmente amparado, até porque, a virtualidade das relações, paradoxalmente, é a realidade hodierna.

1 NOÇÕES PRELIMINARES SOBRE A TELEMÁTICA

De acordo com o Dicionário de Tecnologia (2003), a Telemática pode ser conceituada como a junção de computadores e tecnologias portáteis (meios de telecomunicação), com o objetivo de utilizar e manipular as informações contidas ou geradas a partir desses sistemas.

Na concepção de Gomes e Cervini (1997, p.165), entende-se a Telemática como “a ciência que resguarda a comunicação (transmissão, manipulação) de sinais, dados, escritos, imagens e informações por meio do uso conjunto da informática (do comutador) com as várias formas de telecomunicação”.

O exemplo mais comum e reconhecido de transmissão de informações que utiliza meios tecnológicos é a internet que, nos dias atuais, pode ser acessada dentro de casa, no trabalho, no lazer, na rua, bem como de diversos dispositivos como, por exemplo, do clássico computador pessoal, do *notebook*, do *tablet*, do *smartphone* etc.

No entendimento de Castro (2001, p. 111-112), "a telemática é uma ciência que trata da manipulação de dados e informações, conjugando o computador, sistemas de informática, com os meios de comunicação, telefônicas ou não".

Para a telemática é necessário que se demonstre a combinação dos dois sistemas, pois o que interessa para ela é o tráfego de dados entre um computador, *lato sensu*, e outro, ou vários deles, tendo como veículo o próprio sistema informático ou a rede mundial, por exemplo. Lembrando que não são os únicos sistemas telemáticos possíveis, mas pelo fato de serem os mais comuns e utilizados, guardam a pertinência necessária em questão.

Por sua vez, a interceptação de dados telemáticos busca coletar as informações trafegadas entre sistemas que utilizam a teleinformática, e tem previsão no ordenamento constitucional e infraconstitucional brasileiro, sendo considerado meio legal de prova em processos criminais.

Desse modo, para Capez (2006), caracteriza-se o exercício da interceptação, valendo tanto para a telefônica como para a telemática, o fato de um terceiro, estranho à conversa, se colocar entre o tráfego de dados de outras duas pessoas ou de dois computadores, sem, no entanto, interromper este fluxo, apenas tomando conhecimento do conteúdo, ou seja, sem obstar que a comunicação chegue ao destinatário.

Como forma de maior esclarecimento, mas sem adentrar de modo pormenorizado nas questões técnicas, passamos a diferenciar os dados das informações.

Segundo Oliveira (2002, p. 23), o dado "é qualquer elemento identificado em sua forma bruta, que por si só, não conduz a uma compreensão de determinado fato ou situação", e no caso da informação "é o dado trabalhado que permite ao executor tomar decisões".

No caso da telemática, conclui-se que "informação" é gênero, como transmissão de conhecimento, do qual se tem como espécie o "dado", com a

particularidade de ser eletrônico, tornando-se espécie de informação com emprego de tecnologia.

Mais especificamente aos dados informáticos, Gomes et al. (2000, p. 64) entendem que eles não são decodificáveis aos “olhos simples dos leigos”, ou seja, só poderão ser compreendidos por aqueles que detêm o saber científico em questão.

Quando os Autores acima dizem que os dados informáticos poderão ser decodificados, na verdade eles informam que a decodificação poderá ser manipulada pelos detentores da ciência em voga, pois a tarefa de “traduzir” a informação contida num dado processado ficará a cargo de uma máquina como o computador, por exemplo.

2 BREVE ANÁLISE COMPARATIVA DA LEGISLAÇÃO ESTRANGEIRA SOBRE A INTERCEPTAÇÃO TELEMÁTICA

Apesar da disseminação rápida das modernas ferramentas relacionadas à informática, cada país possui a sua realidade tecnológica e, desta forma, não diferente, é peculiar o tratamento dispensado à questão, desde os procedimentos iniciais de autorização da quebra de sigilo das comunicações, até a maneira com que tratam os infratores que se utilizam dos dados para se comunicarem.

Da mesma forma que no Brasil, em vários outros países, de maneira gradativa e de acordo com os avanços tecnológicos, se verificou a necessidade de incluir a transferência de dados entre duas ou mais pessoas no rol de possibilidades, quando autorizadas, de violação dessa comunicação.

Assim, apesar dos documentos legais estrangeiros já abarcarem as formas tradicionais de comunicação como a correspondência e a telefonia- fixa ou móvel- da mesma forma que as leis e normas brasileiras, eles foram ampliados com o intuito de envolver as comunicações telemáticas ou via internet (UTIMACO *apud* SÍCOLI, 2012, p. 18).

2.1. Nos Estados Unidos

De modo geral, seja ela realizada pelo Estado seja por particulares, a interceptação de dados telemáticos ou de telefonia propriamente dita é considerada

ilegal nos Estados Unidos, ressalvados os casos na esfera do direito penal norte americano, tendo a Corte Judiciária a prerrogativa de supervisionar as interceptações das telecomunicações que porventura forem autorizadas, a requerimento do Ministério Público e Membros do Governo das Agências de Investigação (SHERR et al. *apud* SÍCOLI, 2012. p. 18).

No entanto, paradoxal à regra, após os ataques terroristas de 11 de setembro de 2001, o Congresso dos Estados Unidos da América aprovou um ato mundialmente conhecido como *USA Patriot Act (Ato Pratiótico dos Estados Unidos da América)*[ii], posteriormente assinado pelo presidente do País, onde estabelecia ampla permissão de violação da intimidade, inclusive comunicações telefônicas e tráfego de dados de internet, da pessoa suspeita de práticas terroristas (BANDEIRA, 2005).

Com relação à abrangência das interceptações permitidas nos Estados Unidos não se trata de rol taxativo, pois não são predeterminados para quais espécies de delitos poderá ser autorizada a medida excepcional, além de abranger qualquer comunicação por cabo, verbal ou eletrônica (GARAY, 2012). Assim, inevitavelmente, na visão desse Estado, o direito ao sigilo do indivíduo será sempre mitigado quando, o que estiver em cena, forem os interesses da nação, mesmo que eles não sejam bastante evidentes ou claros suficientes para justificar a irrestrita liberdade na violação ao direito em questão pelo Estado.

2.2. No Chile

A inviolabilidade das comunicações entre os particulares também é garantida no País Chileno, sendo afastada, excepcionalmente, em certas situações admitidas pela legislação. Neste caso, um dos atos mais pertinentes com relação ao tema é o Decreto nº 142 da Subsecretaria de Telecomunicações do Chile, promulgado em 2005, onde está previsto regulamentos acerca da gravação e interceptação de comunicações telefônicas, bem como de outros meios de telecomunicação (SÍCOLI, 2012).

Logo em seu primeiro artigo, o decreto informa que o ato servirá de diretriz procedimental para as empresas prestadoras de serviços de telecomunicação frente aos requerimentos judiciais referentes às interceptações e gravações das conversas (ou tráfego de dados) dos usuários dos serviços em questão.

Com relação às comunicações via internet, o Decreto estabelece que os endereços de *Internet Protocol* (Protocolo de Internet, IP) de determinado provedor de acesso devem ser mantidos atualizados em uma lista, em caráter reservado, à disposição de toda instituição que se encontre permitida a requisitá-la, inclusive o Ministério Público (CHILE, 2005). Da mesma forma, devem manter um registro, não inferior a seis meses, dos históricos de conexão e dados dos seus usuários ou assinantes (CHILE, 2005).

No Código Penal Chileno encontra-se estabelecido, como regra para a interceptação, a anuência da autoridade judicial de forma motivada e sopesando a real necessidade e oportunidade da medida, bem como a proporcionalidade do meio solicitado, norteando-se pelos indícios existentes. Ainda, deverá conter as informações específicas da quantidade de "alvos" interceptados (GARAY, 2012).

Por fim, assim como nos EUA, a abrangência da interceptação (telefônica, telemática, fotográfica e de filmagens, ambiental) é tratada de forma genérica, ou seja, não há rol taxativo dos crimes que dão ensejo a ela. A tarefa de apreciar a possibilidade da medida excepcional incube ao Juiz que se baseará, abstratamente, no que entende como grave delito.

2.3. Na União Europeia

Não há uma legislação única e específica que aborde e regulamente a interceptação telemática em toda a União Europeia, quiçá em todo o Continente Europeu, o que demanda a análise específica dos ordenamentos jurídicos dos países de forma individualizada.

Com relação a acordos internacionais, vale ressaltar a Convenção para combate aos *Cybercrimes* de Budapeste, firmado em 2001, com participação da Europa, Estados Unidos, Japão, Coreia do Sul e Canadá, que tipifica os crimes cometidos com maior frequência na internet e privilegia uma política criminal comum, com a finalidade de tutelar a sociedade contra a incidência de crimes no ciberespaço, através de criação de legislação específica e incentivo à cooperação internacional (TEIXEIRA, 2013, p. 316-317).

Em Portugal há proteção Constitucional à imagem e à intimidade da vida privada, assegurados no artigo 26, nº 1 da Carta (1976), bem como a inviolabilidade do domicílio e da correspondência, consagrada no artigo 34, nº 1 a 4, admitindo a

violação somente em casos excepcionais previstos na lei em matéria de processo criminal. Em relação à comunicação por meio da informática, a Constituição Portuguesa (1976) assegurou previsão e proteção específica no artigo 35, nº 1 a 7, que, além de garantir o acesso aos cidadãos aos dados informatizados ou às redes de informática, igualmente prevê a proibição da violação de informações de terceiros, excepcionando-se somente em situações com previsão legal.

A interceptação das comunicações em Portugal está disciplinada no seu Código de Processo Penal (VERSÃO 2018), mais precisamente no Capítulo IV que trata *"Das escutas Telefónicas"*, compreendendo os artigos 187 a 190. No artigo 189 está disciplinada a abrangência ampliada da lei:

> Artigo 189.º [...]
> 1 - O disposto nos artigos 187.º e 188.º é correspondentemente aplicável às conversações ou comunicações transmitidas por qualquer meio técnico diferente do telefone, designadamente correio electrónico ou outras formas de transmissão de dados por via telemática, mesmo que se encontrem guardadas em suporte digital, e à intercepção das comunicações entre presentes (CÓDIGO DE PROCESSO PENAL PORTUGUÊS, 2018).

O principal requisito para a admissibilidade da ordem de interceptação é a indicação razoável de que há participação em determinados crimes, elencados pela própria Lei, sendo a medida adequada e necessária para a descoberta da verdade ou da prova.

Além disso, preconiza o artigo 188 do mesmo diploma legal que as informações obtidas por meio da interceptação devem ser lavradas em auto e encaminhadas imediatamente ao juiz que autorizou a medida, juntamente com as fitas ou elementos análogos, indicando-se as partes consideradas relevantes para a prova. No entanto, é permitido ao órgão de polícia criminal responsável pela investigação tomar conhecimento prévio do conteúdo interceptado a fim de praticar atos urgentes e necessários à preservação da prova (medidas cautelares, por exemplo).

No Estado Espanhol o cenário legal não se distancia muito dos demais, pois vincula as eventuais restrições aos direitos fundamentais do cidadão à anterior previsão legal ou constitucional, ou seja, as possibilidades devem estar traças e delineadas antes de qualquer violação, o que, via de regra, se vê nos ordenamentos democráticos.

O que chama mais atenção no Código de processo Penal Espanhol (LEY DE ENJUICIAMIENTO CRIMINAL, 1882) é a excepcionalidade trazida pelo artigo 579, item 4, que permite ao Ministro do Interior, ou na ausência deste, ao Diretor de Segurança do Estado, autorizar a interceptação quando se tratar de situações relacionadas à investigação de bandos armados, terroristas e rebeldes. No entanto, é necessário que a medida requeira urgência e que seja confirmada ou revogada pelo juiz, no prazo máximo de 72 horas.

Na Itália, diferentemente das legislações até então mencionadas, a implementação da interceptação telefônica ou telemática pode ser determinada pelo Representante do Ministério Público em caráter emergencial, nas situações de investigação do crime organizado, por exemplo, sem que haja, para tanto, uma ordem judicial (GARAY, 2012). No entanto, de acordo com Garay (2012), a autorização de monitoramento das comunicações deve ser submetida ao judiciário após vinte e quatro horas, conforme determina o artigo 267, inciso II do *Códice di Procedura Penale* (Código de Procedimento Penal, 1988) italiano.

Caso o judiciário entenda não ser plausível a motivação para dar continuidade à medida, poderá declarar a ilegalidade e inutilizar todo o conteúdo monitorado para a utilização como prova (artigo 267, inciso II do *Códice di Procedura Penale*). Importa salientar a existência de um rol exemplificativo dos crimes submetidos à autorização para interceptação, constante no artigo 266 do citado código, dentre eles, crimes cuja pena exceda os cinco anos, delitos que envolvam explosivos, armas, drogas, contrabando e, mais recentemente a pedofilia.

Além disso, o próprio artigo 266, no seu inciso I, menciona a previsão da ferramenta de interceptação telemática, bem como de fluxo de dados entre mais sistemas tecnológicos (COLLI, 2010).

Desta forma, após análise das legislações estrangeiras pertinentes, pode-se notar que, de modo geral, há previsão da interceptação telemática e que ela é aceita como prova na persecução penal, uma vez tratar-se de tipo de comunicação em voga e que, consequentemente, é bastante utilizado para a prática de delitos em todo o mundo.

Consonante, também, é a ideia de que a ferramenta da interceptação do fluxo de dados telemáticos deva ser utilizada somente como exceção, ou seja, a proteção ao sigilo das comunicações deve ser a regra. Há, porém, em algumas normas jurídicas, a flexibilidade da autorização da medida nos casos de crimes mais graves

como o terrorismo, ou a existência de legislações menos protetivas como, por exemplo, a dos Estados Unidos, em que o poder estatal é mais amplo e abrangente, pelos motivos já expostos anteriormente.

3 ASPECTOS CONSTITUCIONAL-NORMATIVOS RELACIONADOS À TELEMÁTICA NO BRASIL

A interceptação de dados telemáticos está prevista na legislação brasileira desde a Lei Fundamental até aos atos normativos mais específicos (Leis Ordinárias, Resoluções, Decretos, etc.), sendo considerado meio legal de prova em processos criminais penais, analisados os requisitos exigidos para a sua autorização.

O sigilo das comunicações, inicialmente somente na forma de correspondências, encontra amparo desde a primeira Constituição do Brasil de 1824, ainda no período Imperial, encontrando previsão, também, nas demais leis fundamentais que se seguiram (CAMPANHOLE; CAMPANHOLE, 2000). No entanto, a previsão de dados que utilizam a telemática, propriamente dita, somente aconteceu na Carta Magna de 1988, na verdade, talvez, por motivos de conhecimento tecnológico relacionado às ferramentas de informática até então.

Não podendo imaginar a dimensão que a informática e a internet tomariam, mesmo que de forma indireta, o Código Brasileiro de Comunicações- Lei 4.117, publicada em 05 de outubro de 1962, com retificação em dezembro do mesmo ano- pode ser considerado o marco inicial da proteção dos dados utilizados através daqueles meios, pois, em seu artigo 55, havia a previsão de que as telecomunicações eram invioláveis. A referida Lei, no tocante aos seus aspectos básicos e essenciais, bem como aos conceitos e preceitos gerais, foi recepcionada pela Constituição de 1988, com ressalva, porém, aos dispositivos que se relacionavam à matéria penal, especialmente o artigo 57, que era bastante abrangente, pois trazia várias exceções à vedação da inviolabilidade das telecomunicações.

A Constituição Federal Brasileira de 1988 estatui no seu Título II os Direitos e Garantias Fundamentais, onde no Capítulo I (Dos Direitos e Deveres Individuais e Coletivos) está esculpido o artigo 5º que, dentre outros relevantes incisos, estabelece o seguinte:

> Art. 5º [...]:
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal (BRASIL, Constituição Federal, 1988).

Desta forma, a simples leitura dos dispositivos supramencionados permite a conclusão de que o Legislador Constituinte Originário intencionava-se pela inviolabilidade do sigilo das comunicações, estabelecendo ele próprio uma exceção, seguindo determinados requisitos. No entanto, uma análise mais aprofundada do inciso XII do artigo 5º da CRFB/1988 gera uma série de questionamentos bastante discutidos pela doutrina brasileira.

No ensinamento de Silva (2006), apesar da má redação do dispositivo, o inciso XII é dividido em dois blocos ou conjuntos, apartados pela partícula *"e"*, e finalizados por uma cláusula de exceção. A partir disso, a primeira disposição trataria do sigilo das correspondências e da telegrafia (ou comunicações telegráficas), à medida que a segunda disposição volveria acerca do sigilo dos dados e das comunicações telefônicas, ficando este bloco abarcado pela expressão *"último caso"* (SILVA, 2006).

Na visão de Greco Filho (1996), compartilhando de pensamento oposto ao primeiro doutrinador, quando o legislador esculpe a expressão supracitada estava pretensioso a abranger somente as comunicações telefônicas, já que, por se tratar de medida excepcional, deve-se dar uma interpretação restritiva à interceptação.

Essa divergência de pensamentos adquire ainda mais força quando se verifica que não se trata apenas de um dispositivo pechoso, de uma redação mal elaborada, gramaticalmente falando, mas, talvez, de controvérsia intencionalmente proposta pelos legisladores. Nesse sentido, para a Grinover (1997), o que houve, de fato, foi a aprovação de texto constitucional diverso do concebido originariamente que determinava que fosse inviolável "o sigilo da correspondência e das comunicações de dados, telegráficas e telefônicas, salvo por ordem judicial, nas hipóteses e na forma que a lei estabelecer, para fins de investigação criminal ou instrução processual". Como se pode notar, não havia a presença das expressões *penal* e *último caso*.

De acordo com o art. 5º, inciso XII da Constituição Federal, havia uma primeira limitação quanto à sua efetivação, pois necessitava de Lei regulamentadora da norma, isto é, uma lei que prescrevesse os casos nos quais seria realizada a interceptação e a forma que esta seria realizada, determinando a amplitude da ferramenta, bem como os prazos e pessoas autorizadas a requererem e a concederem.

A Lei 9.296 foi editada somente em 1996, ou seja, oito anos após a Carta Constitucional, o que gerou inúmeros prejuízos a vários processos nesse ínterim, pois, apesar de terem os pedidos deferidos pelos juízos iniciais- com base no art. 57, II, "e"do Código Brasileiro de Comunicações- as interceptações foram consideradas provas ilícitas pelos Tribunais Superiores, acarretando assim sua nulidade.

Com a edição da Lei, então, restou preenchido o primeiro requisito exigido pela disposição constitucional, que era a normatização legal do procedimento de interceptação. No entanto, o artigo 5º, XII, da Constituição Federal, e o próprio artigo 1º da Lei das Interceptações trazem outros dois requisitos para a autorização da medida cautelar, quais sejam, a dependência de ordem do juiz competente para apreciar o feito principal e a sua utilização para prova em investigação criminal e em instrução processual penal.

Dessas duas exigências extraem-se algumas conclusões. A primeira delas é de que a Lei foi mais rigorosa do que a Constituição em relação ao requisito da autorização judicial, pois a Carta Magna apenas exigia que a concessão da medida fosse realizada por autoridade judiciária, não especificando a necessidade de que fosse pelo "juiz competente da ação principal" (artigo 1º, Caput, "in fine"), feito pela Lei 9296/1996.

Outra conclusão extraída, agora com relação à utilização da prova, é de que a interceptação está restrita à esfera criminal, seja na fase pré-processual, em que serão realizadas as investigações, com o intuito de se descobrir a autoria e a materialidade de determinado crime, seja na instrução da ação penal. Desta forma, os juízes de assuntos cíveis ou de família, como tantos outros, ressalvado o plantão judiciário, não podem figurar como autorizadores da medida de interceptação, nem esta ser iniciada em vara judicial estranha à criminal (GOMES; MACIEL, 2011).

Nada impede, porém, a utilização da interceptação, nas suas diversas formas, como prova emprestada em processo diverso do criminal. Segundo o Supremo Tribunal Federal (Inquérito 2424-RJ[iii]), corroborado pelo Superior Tribunal

de Justiça, isso poderá ocorrer até mesmo em processo administrativo disciplinar, sendo, neste último caso, contra servidores públicos que constavam como réus no processo criminal que ensejou a medida cautelar utilizada como prova.

A lei 9.296/1996 é conhecida, no mundo jurídico, como "Lei das Interceptações Telefônicas", porém, além destas, versa sobre os procedimentos de interceptação de comunicações que utilizam como substrato o sistema de telemática e informática, através do fluxo de dados, apesar de diversas vezes só ser mencionado a telefonia. Essa inclusão se comprova, expressamente, na análise do artigo 1º, Parágrafo Único, da referida Lei. Assim, portanto, há de se observar na execução da interceptação telemática todas as formalidades exigidas à de telefonia, inclusive a de que a medida seja utilizada de forma excepcional, ou seja, somente quando não houver possibilidade da produção de prova por outro meio senão pela violação da intimidade em questão (artigo 2º, II), além de ver respeitado o prazo de quinze dias para a execução da medida, que pode ser renovado caso se comprove a indispensabilidade do meio de prova (Artigo 5º), dentre várias outras exigências contidas no texto legal (GOMES e MACIEL, 2011).

Apesar do longo tempo que o legislador levou para a edição da Lei de Interceptação, esta não foi capaz de sanar todos os problemas que a falta de regulamentação trazia, bem como não podia prevê todas as novas possibilidades de comunicação e tráfego de dados que passariam a existir. Com isso, foram surgindo ao longo dos anos outras Leis e regulamentos a fim de cuidarem, minuciosamente, do assunto, tais como a Lei das Telecomunicações (9.472/1997), Resoluções da ANATEL (Agência Nacional de Telecomunicações), Resoluções do CNJ e CNMP, Portaria nº 22 da Secretaria Nacional de Segurança Pública, Lei 12.737 (tipificação de delitos informáticos) e a Lei 12.965 (o Marco Civil da Internet). O objetivo deste estudo não é esgotar as disposições acerca do tema trazidas por essas normas, assim, não se adentrará especificamente em cada uma delas, mas vale o seu registro para futuras análises.

Resta claro, portanto, que a discussão de estabelecer menor ou maior amplitude da interceptação telemática, bem como regulamentá-la com mais ou menos rigor, está longe de ser um assunto pacífico, visto que, encontram-se pelo caminho interesses diversos, sejam para dar mais força ao poder de punir estatal – para os que defendem maior abrangência a cautelar –, sejam para diminuir a capacidade e a eficácia punitiva da ferramenta.

4 INTERCEPTAÇÃO TELEMÁTICA E SUA FORÇA PROBANTE

A grande questão que envolve a medida excepcional da interceptação telemática é a sua capacidade de se constituir como meio de prova no ambiente processual, bem como sua abrangência como objeto de convicção do magistrado. Nesse sentido, importa o enveredamento pelo estudo do instituto das provas no que concerne à persecução criminal, estabelecendo, principalmente, o alcance e os limites processuais da prova produzida a partir da interceptação de dados telemáticos, vez que se trata de ferramenta consideravelmente nova e que requer certo domínio técnico e, por isso, ainda demanda discussão e análise.

Conceituada como sendo um conjunto de atos praticados pelos envolvidos no processo (as partes, o magistrado e determinados terceiros), seja direta ou indiretamente, a "prova", com finalidade de demonstrar a veracidade ou a falsidade de um fato, é o sustentáculo processual capaz de levar a convicção à autoridade judicial e, consequentemente, ao melhor (e justo) resultado da causa. Nas palavras do Professor Fernando Capez, "as provas constituem os olhos do processo" (CAPEZ, 2008. p. 290).

É salutar, porém, distinguir as provas dos elementos informativos, estes colhidos na fase investigatória ou pré-processual, não necessitando da observância do contraditório e da ampla defesa, servindo como subsídio para decretação de Medidas Cautelares- a própria interceptação telemática, por exemplo- e como auxílio para embasamento da ação penal a ser proposta pelo Representante do Ministério Público.

Para o Direito Processual Penal, não muito diferente das demais ciências jurídicas, a prova se fundamenta como elemento instrumental para que as partes busquem a convicção do juiz e, em contrapartida, o meio de que este se serve para analisar os fatos em que os envolvidos fundamentam suas proposições.

Desta forma, demonstra Mirabete (2000, p. 257) que o

> objeto da prova é o que se deve demonstrar, ou seja, aquilo sobre o que o juiz deve adquirir o conhecimento necessário para resolver o litígio. Abrange, portanto, não só o fato criminoso e sua autoria, como todas as circunstâncias objetivas e subjetivas que possam influir na responsabilidade penal e na fixação da pena ou na imposição de medida de segurança.

Os meios probatórios existentes no ordenamento jurídico brasileiro – testemunhas, documentos, perícia, etc. – caminham sempre no mesmo sentido e para o mesmo objetivo, qual seja a mencionada convicção do magistrado. E, na pretensão de alcançá-la, são constituídas provas por vezes comuns, como a documental ou testemunhal, e outras complexas e excepcionais, como a "quebra" de informações sigilosas ou interceptação das comunicações.

Considerada medida de "ultima ratio" (GRINOVER, 1997), a Interceptação telemática- manipulação de dados e utilização de informações através do uso, conjunto ou não, do computador e meios de telecomunicação- começa a tomar proporções, até pouco tempo, inimagináveis, sendo utilizada como meio para se alcançar a peça probatória ou como prova propriamente dita numa instrução processual.

Importante mencionar é que a implementação da Interceptação de Dados Telemáticos está condicionada, dentre outros requisitos, à impossibilidade de se obter os mesmos resultados por outra forma probatória. Esta imposição demonstra que a medida em questão é extremada, e sendo desse modo, suscita vários questionamentos, até porque, ainda, é uma ferramenta consideravelmente nova.

Desta forma, não fugindo à regra, a prova obtida através da interceptação das comunicações telemáticas deve estar condizente com todo o ordenamento jurídico pátrio, ou seja, obediente aos princípios constitucionais e fiel aos mandamentos legais.

Tratando-se de telemática, assim como as outras formas de interceptação mencionadas na lei específica, outros requisitos devem ser observados para que o caráter probatório seja idôneo, os denominados requisitos legais, com expressa previsão no artigo 2º da Lei das Interceptações que, na verdade, preconiza a inadmissibilidade da medida em determinadas situações. Assim, de acordo com o dispositivo legal em questão, será inadmissível a interceptação dos dados telemáticos quando sobrevier qualquer uma das três hipóteses elencadas nos seus incisos e, em razão contrária, entende-se por aceitável a decretação da cautelar quando: forem razoáveis os indícios de autoria ou participação em infração penal; que a interceptação se constitua no único meio de investigação capaz de captar a prova; e que a infração penal caracterizadora do fato seja punível com reclusão.

No que concerne ao primeiro requisito para a concessão da interceptação de dados telemáticos, deve-se atentar para as exigências do *fumus boni iuris (fumaça*

do bom direito) e do *periculum in mora* (perigo na demora), pressupostos indispensáveis para a decretação de medida de natureza cautelar. Para Gomes e Cervini (1997), a exigência do *fumus boni iuris* está relacionada a duas situações, quais sejam: que seja provável a ocorrência autoral do agente criminoso ou sua participação no delito; e que haja igual probabilidade de ter ocorrido a infração penal, isto é, que haja indícios de materialidade. Referindo-se ao *periculum in mora*, Avolio (2010) entende que o que se analisa é a possibilidade de restar prejudicada toda a persecução penal caso a ordem judicial de concessão da interceptação telemática não seja autorizada, podendo trazer risco considerável à instrução processual ou mesmo antes, na fase investigatória.

Desta forma, é imprescindível atentar que a Lei das Interceptações não guardou à interceptação mera suposição ou suspeição baseada em questões subjetivas, muito pelo contrário, o que se espera da existência de indícios é um mínimo de certeza da ocorrência do delito e da autoria que, por sinal, será comprovada com a medida cautelar em voga.

Por outro lado, a concessão judicial para realização da interceptação telemática, da mesma forma que para a telefônica, é revestida de natureza excepcional, isto é, somente se autorizará a medida cautelar em determinadas situações delimitadas pela Constituição Federal e pela legislação infraconstitucional. Para Fernandes (2007), a interceptação – neste momento elencada somente a telefônica, mas, de certo, valendo para a telemática – somente poderá ser autorizada se for considerada como a única forma possível de se evidenciar a autoria e a materialidade do delito, cuja não realização prejudicará o colhimento de elemento de prova importante para a investigação e, consequentemente, para o processo. O mesmo entendimento possui Badaró (2008) que defende só ser possível conceber a interceptação quando demonstrada a impossibilidade dos órgãos de investigação realizar os trabalhos, com tal finalidade, por diferentes formas disponíveis, tais como a colaboração de testemunhas, o reconhecimento pessoal, a busca e apreensão.

Assim, torna-se claro que a intenção do constituinte e do legislador em dar à medida cautelar em discussão um caráter de excepcionalidade nada mais foi que garantir, como regra, a inviolabilidade do sigilo das comunicações, ou seja, a ferramenta deve ser a última razão dos trabalhos investigativos, porquanto devem

ser esgotados, primeiramente, meios disponíveis que tragam menor prejuízo a direitos constitucionalmente protegidos.

Em relação ao último requisito é necessário distinguir a inadmissibilidade da interceptação especificamente para crimes punidos com detenção da utilização daquela medida como prova nos crimes dessa natureza. O que a normatização legal pretendeu impedir é que a investigação de um fato punível, no máximo, com pena de detenção, dê ensejo à decretação de ordem judicial autorizando o afastamento do sigilo das comunicações telemáticas, não impedindo, porém, que a prova seja utilizada no caso do crime ser conexo com outro punido com pena de reclusão, para o qual foi permitida, legalmente, a interceptação (GOMES; MACIEL, 2011).

A mesma ideia vale para o encontro fortuito de novos delitos e novos criminosos, no entanto, agora, com relação a crimes apenados com reclusão, ocorrido a partir de interceptação que, inicialmente, não foi a eles direcionada. Assim, conforme Gomes e Maciel (2011), os Tribunais reservam o mesmo entendimento majoritário discorrido até o presente, ou seja, também exigem a conexão do novo crime com o delito que determinou a ordem judicial da cautelar.

Desta forma, as interceptações de dados telemáticos, uma vez legalmente disciplinadas e efetuadas com estrita observância dos requisitos impostos no ordenamento jurídico, são aceitas como provas lícitas, sendo admissível seu resultado como fonte probante no processo, conforme entendimento da doutrina e da jurisprudência. Não se questiona sua licitude quando amparada pelos preceitos constitucionais e legais, restando evidente sua total utilização quando obedecido os requisitos que autorizam seu pedido e sua concessão.

Contudo, por tratar-se de medida consideravelmente nova e que utiliza em sua estrutura a tecnologia, a medida de exceção em voga guarda peculiaridades que não se verifica na interceptação telefônica propriamente dita como, por exemplo, a dificuldade em se obter a identidade do criminoso que utiliza equipamentos informatizados para cometer delitos.

CONSIDERAÇÕES FINAIS

A necessidade do sistema jurídico se abrir aos anseios de uma sociedade que, constantemente, se encontra em processo evolutivo é latente e inquestionável,

visto que o que se espera é uma resposta adequada e eficiente das normas em relação às condutas humanas, hoje, mais do que nunca, influenciadas pela tecnologia.

Pode-se perceber que a crescente informatização das operações realizadas pelo indivíduo ou por uma coletividade proporciona aos usuários de má-fé o desenvolvimento de instrumentos capazes de gerar prejuízos em diversas esferas, seja econômica- nos crimes direcionados às transações bancárias via internet ou ao comércio eletrônico- seja pessoal ou social, principalmente nos delitos ligados à privacidade ou à honra e relacionados à pedofilia e a pornografia infantil, por exemplo.

O que mais preocupa os órgãos responsáveis pela investigação criminal e pela persecução penal como um todo é a maneira mais eficaz e contundente de se chegar ao possível autor do cybercrime, visto que a tecnologia, da mesma forma que traz benefícios aos usuários, é sinônima de barreira à constituição do documento eletrônico como prova, pois se encontra em constante modificação.

Ficou constatado que, de forma geral, a medida cautelar da interceptação telemática pode materializar-se em prova idônea no processo penal brasileiro, desde que constituída de legalidade, ou seja, desde que atendidos todos os requisitos estabelecidos pelo ordenamento jurídico, em especial da Lei 9.296/1996 que regula o inciso XII, do artigo 5º, da Constituição Federal.

Assim, o entendimento de que a comunicação através de dados estaria amparada pelo sigilo absoluto, como entende a minoria doutrinária, hodiernamente não é defendida pelos julgadores e nem pela doutrina majoritária, pois, além de entenderem não haver direito inquebrantável, compartilham da ideia de que a interpretação a ser dada à parte final do dispositivo constitucional mencionado é no sentido de incluir os dados na exceção que prevê o afastamento do sigilo.

A internet é, sem dúvida, um avanço na democratização do acesso à informação e, devido a isso, sua disseminação é bastante estimulada. Assim, seu uso responsável, condizente com as normas sociais da comunidade virtual e com o ordenamento jurídico, é imprescindível, tanto para garantir a própria segurança do usuário quanto a dos demais na grande rede mundial.

Portanto, regulamentar as relações virtuais não é sinônimo de tirania digital, não se pretende, de maneira alguma, retirar a essência da internet que é, exatamente, a manifestação democrática das opiniões, no entanto, não se pode

conceber que um ambiente, onde estão evidentes vários institutos como, por exemplo, a intimidade, a honra, o patrimônio, dentre vários outros, fique relegado. A liberdade total, além de dificultar a investigação, pois não cria responsabilidades aos usuários e aos provedores, cria a sensação de que “tudo pode” no meio virtual, incentivando, de certa forma, que os cibercriminosos continuem a praticar suas condutas maliciosas, pois a constituição da prova de que ele é o autor do crime será, demasiadamente, difícil.

ASPECTOS CONSTITUCIONALES Y PENAIS DE LA INTERCEPCIÓN TELEMÁTICA: su fuerza probante

RESUMEN

Los medios informatizados, especialmente la red mundial de ordenadores, a menudo se utilizan para la comisión de crímenes que, por sus características peculiares, son de difícil investigación. El presente estudio tiene por finalidad el análisis constitucional y penal de la prueba obtenida por la interceptación de datos telemáticos, demostrando la forma en que se produce y se utiliza en la investigación policial y en la fase procesal. En la ausencia de una norma específica, varias situaciones que permean la materia quedan oscuras, entre ellas la posibilidad o no de la medida cautelar se constituye como prueba idónea en el proceso, pero, sobre todo, lo que más se indaga es cómo hacer viable la reglamentación del mundo virtual. En cuanto a la primera cuestión, es mayoritario el entendimiento de ser perfectamente aceptable la interceptación telemática como instrumento probatorio, desde que amparada por el manto constitucional y legal. En cuanto a la segunda, no hay consenso entre los usuarios y la doctrina, ya que la normatización, para los primeros, sería mitigar la libertad en el ambiente virtual, contrariando la esencia misma de éste, pero para los adoctrinadores -con algunas divergencias- y especialmente el Poder Público, es necesario y urgente, pues los cybercrimes crecen vertiginosamente, pidiendo pronta enfrentamiento por parte del Estado. Se trata de una investigación de naturaleza básica; exploratoria, en cuanto a los objetivos; cualitativa, en relación con el enfoque; y bibliográfica, en cuanto a los procedimientos metodológicos.

Palavras clave: Secreto de las comunicaciones. Interceptación Telemática. Prueba.

REFERÊNCIAS

AVOLIO, L. F. T. **Provas ilícitas: interceptações telefônicas, ambientais e gravações clandestinas**. 4. ed. São Paulo: Revista dos Tribunais, 2010.

BADARÓ, Gustavo H. R. Ivahy. **Direito processual penal**. Rio de Janeiro: Elsevier, 2008.

BANDEIRA, L. A. M. **Formação do Império Americano: da guerra contra a Espanha à guerra no Iraque**. Rio de Janeiro: Civilização Brasileira, 2005.

BRASIL. **Código Brasileiro de Comunicações - Lei nº 4.117**. Presidência da República. Brasília: 1962.

BRASIL. **Constituição Federal de 1988**. Presidência da República. Brasília: 1988.

BRASIL. **Lei nº 9296**. Presidência da República. Brasília: 1996.

CAMPANHOLE, Hilton Lobo; CAMPANHOLE, Adriano. **Constituições do Brasil**. 14.ed. São Paulo: Atlas, 2000.

CAPEZ, Fernando. **Curso de Direito Penal: legislação penal especial**. V.4. São Paulo: Saraiva, 2006.

CAPEZ, Fernando. **Curso de processo penal**. 15ª ed. Revisada e atual. São Paulo: Saraiva, 2008.

CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus aspectos processuais**. Rio de Janeiro: Editora Lúmen Júris, 2001.

CHILE. **Decreto 142: Reglamento Sobre Interceptación y Grabación de Comunicaciones Telefónicas y de Otras Formas de Telecomunicación. Biblioteca Del Congresso Nacional do Chile**. Disponível em: <http://www.leychile.cl>. Acesso em: 07 jun. 2018.

COLLI, Maciel. Interceptações telefônicas: uma análise sob o direito comparado da Itália, Espanha e Portugal. In: Nereu José GIACOMOLLI, N. J.; André Machado MAYA, A. M. (org.) **Processo penal contemporâneo**. Porto Alegre: Núria Fabris, 2010.

DICIONÁRIO DE TECNOLOGIA. São Paulo: Ed. Futura, 2003.

ESPANHA. **Ley de Enjuiciamiento Criminal**. Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-1882-6036>. Acesso em: 27 jun. 2018.

FERNANDES, Antonio Scarance. **Processo penal constitucional**. 5. ed. São Paulo: Revista dos Tribunais, 2007.

GARAY, Humberto de Sá. **Interceptação Telefônica no Brasil: (Des) Entendimentos e formação da prova**. Rio Grande do Sul: PUCRS, 2012.

GOMES, Abel Fernandes et al. **Crime organizado e as suas conexões com o Poder Público: comentários a Lei nº 9.034/95**. Rio de Janeiro: Impetus, 2000.

GOMES, Luiz Flávio. **Interceptação Telefônica – Serendipidade é aceita pelo STJ**. (2001). Disponível em: <www.atualidadesdodireito.com.br>. Acesso em: 28 jun. 2018.

GOMES, Luiz Flavio; CERVINI, Raúl. **Interceptação telefônica: lei 9.296, de 24.07.96**. São Paulo: Editora Revista dos Tribunais, 1997.

GOMES, Luiz Flávio; MACIEL, Silvio. **Interceptação telefônica: comentários à Lei 9.296, de 24.07.96**. São Paulo: Revista dos Tribunais, 2011.

GRECO FILHO, Vicente. **Interceptação Telefônica: Considerações sobre a Lei 9.296, de 24 de julho de 1996.** São Paulo: Saraiva, 1996.

GRINOVER, Ada Pellegrini; FERNANDES, Antonio Scarance. **As Nulidades no Processo Penal**. 6ª edição. São Paulo: Revista dos Tribunais, 1997.

ITÁLIA. **Códice de Procedura Penale**. Disponível em: <http://www.brocardi.it/codice-di-procedura-penale/libro-terzo/titolo-iii/capo-iv/art267.html>. Acesso em: 21 jun. 2018.

MIRABETE, Julio Fabbrini. **Processo Penal**. 10.ed. Edição. São Paulo: Editora Atlas, S.A. 2000.

OLIVEIRA, Djalma Pinheiro Rebouças de. **Sistema de informações gerenciais**. 8.ed. São Paulo: Atlas, 2002.

PORTUGAL. **Código De Processo Penal**. Disponível em: <http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?ficha=101&artigo_id=&nid=199&pagina=2&tabela=leis&nversao=>. Acesso em: 20 jun. 2018.

PORTUGAL. **Constituição da República Portuguesa**. Disponível em: <http://www.tribunalconstitucional.pt/tc/crp.html>. Acesso em: 20 jun. 2018.

SÍCOLI, Fábio Caús. **Uma proposta de modelo para transmissão de dados interceptados na Internet brasileira**. Brasília/DF: 2012.

SILVA, José Afonso da. **Comentário Contextual à Constituição**. 2.ed. São Paulo: Malheiros, 2006.

TEIXEIRA, Tarcisio. **Curso de direito e processo eletrônico: doutrina, jurisprudência e prática**. São Paulo: Saraiva, 2013.

[i] Neste ponto se fala de uma regulamentação de fato, intervencionista, isto é, não apenas principiológica ou dogmática, como pretendeu a Lei 12.965, de 23 de abril de 2014, o chamado "marco civil da internet no Brasil".

[ii] Notícia disponível em: http://exame.abril.com.br/economia/noticias/congresso-dos-eua-prorroga-lei-antiterrorista-patriot-act-2 Acesso em: 05 fevereiro 2018.

[iii] Disponível em: <http://www.stf.jus.br/portal/jurisprudencia/visualizarEmenta.asp?s1=000089005&base=base Acordaos> Acesso em: 05 jul. 2018.