RICARDO SIDI MACHADO DA SILVA

A interceptação das comunicações telemáticas no processo penal

Dissertação de Mestrado

Orientador: Prof. Dr. Marcos Alexandre Coelho Zilli

Faculdade de Direito da Universidade de São Paulo
São Paulo
2014

RICARDO SIDI MACHADO DA SILVA

A interceptação das comunicações telemáticas no processo penal

Dissertação apresentada à Faculdade de Direito da Universidade de São Paulo para a obtenção do título de Mestre em Direito.

Área de concentração: Direito Processual

Orientador: Prof. Dr. Marcos Alexandre Coelho Zilli

São Paulo
2014

Nome: SILVA, Ricardo Sidi Machado da
Título: A interceptação das comunicações telemáticas no processo penal

Dissertação apresentada à Faculdade de Direito da Universidade de São Paulo para a obtenção do título de Mestre em Direito.

Área de concentração: Direito Processual

Aprovado em: ____/____/_____

Banca Examinadora:

Prof. Dr. Marcos Alexandre Coelho Zilli

Instituição: Universidade de São Paulo

Julgamento: _____ Assinatura: _____

_____

Instituição: _____

Julgamento: _____ Assinatura: _____

Prof. _____

Instituição: _____

Julgamento: _____ Assinatura: _____

RESUMO

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

A Constituição brasileira de 1988 estabeleceu o direito à inviolabilidade da intimidade, da vida privada e do sigilo das comunicações, apresentando-se os dois primeiros como princípios e o último como regra. A regra da inviolabilidade do sigilo das comunicações se fez acompanhar de cláusula de exceção pela qual o constituinte admitiu hipóteses de restrição a esse direito, notadamente para fins de investigação criminal ou instrução processual penal, nas hipóteses e na forma que a lei estabelecer. Uma das formas de restrição vem a ser a interceptação das comunicações telemáticas, que o trabalho se propõe a analisar, de modo a verificar os limites da atuação estatal no uso desse método de investigação. Em tal análise, de modo a definir o âmbito de proteção dos direitos acima citados, o autor considera, além dos dispositivos da Constituição e legislação brasileiras, convenções internacionais de direitos humanos e a interpretação que lhes é dada por cortes regionais de direitos humanos e adota, como critérios e métodos, o princípio da proporcionalidade, os padrões doutrinariamente concebidos para a construção de um processo penal que se aproxime de uma meta de eficiência e garantismo e as experiências de outros países pesquisados.

Palavras-chave: Interceptação. Comunicações. Telemáticas.

ABSTRACT

SILVA, R. S. M. **The interception of electronic communications at criminal procedure law**. 266 f. Dissertação (mestrado) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2014.

The Brazilian Constitution of 1988 established the rights to inviolability of intimacy, privacy and confidentiality of communications, presenting the first two as principles and the last one as a rule. The rule of the inviolability of the secrecy of communications was followed by an exception clause which specifies the hypotheses in which such right may be restricted, notably for purposes of criminal investigation or criminal procedure, in the cases and in the form provided by statutory law. One of the possibilities of such restriction is the interception of electronic communications, which this paper aims to analyze in order to verify the limits for state action in the use of such criminal investigation method. In such analysis, in order to define the scope of protection of the abovementioned right, the author considers, in addition to the provisions set forth in the Brazilian Constitution and law, international human rights conventions and their interpretation given and adopted by regional human rights courts, and, as criteria and methods, the principle of proportionality, the doctrinally conceived standards for the construction of a criminal procedure system closer to an objective of efficiency and fundamental individual rights protection, as well as the experiences of other researched countries.

Keywords: Monitoring. Wiretapping. Eavesdropping. Surveillance. Electronic. Communications. Interception.

LISTA DE SIGLAS

ABIN	Agência Brasileira de Inteligência
ABNT	Associação Brasileira de Normas Técnicas
CADH	Convenção Americana de Direitos Humanos
CEDH	Convenção Europeia para a Proteção aos Direitos Humanos
CF	Constituição da República Federativa do Brasil de 1988
Corte IDH	Corte Interamericana de Direitos Humanos
CPC	Código de Processo Civil
CPI	Comissão Parlamentar de Inquérito
CPP	Código de Processo Penal
DUDH	Declaração Universal dos Direitos Humanos
GCHQ	*Government Communications Headquarters*
IMEI	*International Mobile Equipment Identifier*
IMSI	*International Mobile Subscriber Identity*
IOCA	*Interception of Communication Act de 1985*
IPT	*The Investigatory Powers Tribunal*
LC	Lei Complementar
NIST	*National Institute of Standards and Technology*
NSA	*National Security Agency*
RIPA	*Regulation of Investigatory Powers Act 2000*
STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
TCE	*Tribunal Constitucional de España*
TEDH	Tribunal Europeu de Direitos Humanos
USC	*United States Code*

SUMÁRIO

INTRODUÇÃO

O presente trabalho se propõe a analisar tema atual e sobre o qual tantas dúvidas ainda pairam, tanto no que se refere à possibilidade jurídica que o Estado tem de restringir o sigilo das comunicações dos indivíduos e em que medida, quanto no que se refere à possibilidade técnica de se monitorar o conteúdo das comunicações, realizadas hoje através dos mais diversos e variados meios tecnológicos que surgem dia após dia[1].

A relevância do tema se mostra muito bem ilustrada em passagem da obra do espanhol Oscar Morales García (2003), para quem a expansão da tecnologia nos meios de comunicação contribui com o processo de globalização econômica e cultural, mas, ao mesmo tempo, abre portas para novas formas de vulneração de bens jurídicos, na medida em que o próprio mecanismo de transmissão de dados se torna um setor de risco[2]. Mais do que isso, tal expansão transforma as relações sociais de um modo impressionante, notável, por exemplo, no fato de que a confidencialidade de mensagens criptografadas e a possibilidade de certificar a identidade de seu emissor são bem mais seguras do que os sistemas atuais, a ponto de estimular uma reflexão sobre o próprio sistema democrático de eleição de representantes. Chega-se a falar em "democracia eletrônica", apontando para um novo modo de participação popular nos rumos de um governo, não só na eleição de governantes, mas na própria tomada de decisões[3]. E, se os próprios fundamentos do Estado se alteram significativamente diante de tecnologias capazes de estabelecer comunicação com todo o planeta em tempo real, as relações sociais primárias sofrem o mesmo efeito[4].

Esse fenômeno gera um aumento na necessidade de tutela, inclusive penal, das bases do novo sistema organizacional, quais sejam, tráfego de dados, segurança das transações comerciais, prevenção de danos nos centros de comunicações individuais e coletivas das empresas. Os criminosos comuns, ou seja, aqueles que atentam contra bens jurídicos outros

---

[1] O presente trabalho obedece à norma da Associação Brasileira de Normas Técnicas indicada no *site* da Universidade de São Paulo (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Diretrizes para apresentação de dissertações e teses da USP**: documento eletrônico ou impresso – Parte I (ABNT). 2ª ed. rev. e ampl. São Paulo: Sistema Integrado de Bibliotecas da USP, 2009. Disponível em: <http://www.teses.usp.br/index.php?option=com_content&view=article&id=52&Itemid=67&lang=pt-br>. Acesso em: 09 jan. 2014), bem como à Resolução FD/PÓS nº 01/2002, da Comissão de Pós-graduação da Faculdade de Direito da Universidade de São Paulo (Disponível em: <http://www.direito.usp.br/pos/arquivos/Resolucao_FD_POS_N1_2002.pdf>. Acesso em: 09 jan. 2014).

[2] GARCÍA, Oscar Morales. Seguridad en las redes telemáticas de comunicaciones: la tensión libertad versus control en la política criminal internacional. In: DA AGRA, Cândido et al. (Org.). **La seguridad en la sociedad del riesgo**: un debate aberto, p. 137/153. Madrid: Atelier, 2003, p. 137.

[3] Ibid., p. 138.

[4] Ibid., p. 138.

que não os cibernéticos[5], naturalmente, também não ficaram alheios aos avanços da tecnologia da informação e comunicação, tendo-se beneficiado com o salto qualitativo que lhes proporcionou essa evolução. A internet, que veio a modificar os mais simples hábitos humanos, permite que qualquer um veja e se comunique com o vizinho em frente à sua janela que permanece mergulhado no seu computador, pelo que se observa que a proximidade cibernética deu lugar ao distanciamento físico-existencial[6]. A internet criou um espaço onde todos colocam os pés na ânsia de apropriação de um pedaço de informação. É um espaço em que ocorre a comunicação entre dispositivos eletrônico-digitais físicos, como roteadores, cabos, modems e antenas, possibilitada por softwares, de navegação, de e-mail, de FTP (*file transfer protocol*) e outros, em que o verdadeiro dá lugar ao mundo dos *bits*, a uma realidade paralela, inaugurando-se uma verdadeira era dos "fluxos informacionais e comunicacionais"[7].

Além da tutela penal, o mesmo avanço tecnológico transforma os meios modernos de comunicação, que vivem em constante evolução, num ponto sensível para o processo penal, na medida em que, por um lado, faz surgir para o Estado a necessidade de contar com métodos persecutórios aptos a lidar com essa modernidade, dentre os quais a interceptação das comunicações telemáticas, por outro, faz surgir, também, a necessidade de se estabelecerem limites cuidadosos a essa atividade persecutória estatal, de modo a que não se admitam, diante de um discurso de crescimento da criminalidade organizada e violenta, violações às garantias fundamentais. É com essa preocupação que se passa a analisar *A interceptação das comunicações telemáticas no processo penal*.

O capítulo 1, "Intimidade, vida privada e interceptação das comunicações telemáticas", se propõe a conceituar e distinguir intimidade e vida privada, demonstrando o surgimento e a evolução desses direitos fundamentais, bem como a verificar a extensão que lhes vêm atribuindo o Tribunal Europeu de Direitos Humanos (TEDH) e a Corte Interamericana de Direitos Humanos (Corte IDH).

Feito isso, o capítulo analisa as formas de resolução da colisão entre o interesse estatal na busca da verdade e o direito do indivíduo à preservação de sua intimidade e vida privada,

---

[5] Segundo o Dicionário Aurélio, cibernética é a ciência que estuda as comunicações e o sistema de controle não só nos organismos vivos, mas também nas máquinas. Do gr. *kybernetiké*, *i. e.*, *téchne kybernetiké*, 'a arte do piloto' (Novo Dicionário Eletrônico Aurélio, versão 7.0., 5ª. ed.). Modernamente, no entanto, o termo se refere a tudo que seja relativo à internet ou à informática. O *Wireless Dictionary* definiu *Cybercrime* como "any act or omission of a responsible action using the internet that makes a person subject to criminal punishment by law" ou, em tradução livre, qualquer ato ou omissão usando a internet que sujeite o responsável a uma punição legal criminal. (WIRELESS Dictionary. Disponível em: <http://www.wirelessdictionary.com/aw_dictionary_widget_wireless.asp>. Acesso em: 12 jul. 2013.)

[6] RODRIGUES, Benjamim Silva. **A monitorização dos fluxos informacionais e comunicacionais**. v. I. Coimbra: Coimbra Editora, 2009, p. 20/21.

[7] Ibid., p. 21/22.

bem como o binômio eficiência e garantismo e o princípio da proporcionalidade, como premissas e critérios a embasar essa análise.

O capítulo 2, de nome "Comunicação telemática, internet e os meios modernos de interceptação", tratará de conceitos básicos da área de telecomunicações, de modo a viabilizar a compreensão de expressões empregadas nos precedentes jurisprudenciais analisados no trabalho. O mesmo capítulo buscará desmistificar o universo dos meios modernos de interceptação telemática, cumprindo ressaltar a dificuldade de acesso a fontes de pesquisa.

Note-se, nesse sentido, que o relatório anual entregue ao parlamento britânico pelo Comissário de Interceptações de Comunicações em 2012, ao descrever, por força de lei[8], as atividades oficiais de interceptação realizadas no país ao longo daquele ano, ressalvou, como fez nos anos anteriores, que não se estava incluindo exemplos detalhados das operações das agências de inteligência para que a segurança nacional não restasse prejudicada[9].

Quando do vazamento de documentos sigilosos pelo ex-técnico da CIA Edward Snowden, que revelaram minúcias sobre os métodos de espionagem digital que agências de inteligência norte-americanas e inglesas têm adotado, três grandes veículos de imprensa, precisamente *The Guardian*, *The New York Times* e *ProPublica*, concluíam um trabalho conjunto de reportagem sobre o assunto, no que foram surpreendidos por agentes de inteligência que lhes solicitaram a suspensão da publicação, sob pena de acabar por alertar alvos estrangeiros e instigá-los a mudar seus métodos de comunicação e criptografia, de modo a tornar mais difícil sua interceptação ou decifração[10].

As duas colocações acima ilustram bem a razão para a escassez de fontes de pesquisa capazes de subsidiar a construção do capítulo 2, pois os equipamentos, os softwares, as tecnologias, os métodos enfim, empregados na interceptação de comunicações são temas restritos a um grupo fechado de profissionais ligados à segurança pública, a agências de

---

[8] RIPA 2000. *Section* 58(4) As soon as practicable after the end of each calendar year, the Interception of Communications Commissioner shall make a report to the Prime Minister with respect to the carrying out of that Commissioner's functions. (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/pdfs/ukpga_20000023_en.pdf>. Acesso em 15 ago. 2013).

[9] 2012 Annual Report of the Interception of Communications Commissioner: Presented to Parliament pursuant to Section 58(6) of the Regulation of Investigatory Powers Act 2000, The Stationery Office Limited, London, 2013, p. 8: "The following case summaries are just a sample of a large number of operations that have been examined during the 2012 inspections where lawful interception and/or communications data have played a role in a successful outcome. I have, as in previous years, not provided detailed examples of operations from the intelligence agencies in order not to prejudice national security." (Disponível em: <http://www.iocco-uk.info/docs/2012%20Annual%20Report%20of%20the%20Interception%20of%20Communications%20Commissioner%20WEB.pdf>. Acesso em: 01 set. 2013).

[10] BUCHANAN, Matt. How the N.S.A. Cracked the Web. **The New Yorker**. 07 set. 2013. Disponível em: <http://www.newyorker.com/online/blogs/elements/2013/09/the-nsa-versus-encryption.html>. Acesso em: 06 ago. 2013.

inteligência e até a setores específicos de empresas de comunicações, que, apesar de privadas, se apresentam como departamentos igualmente impenetráveis e inacessíveis.

Acrescenta-se que, quando o autor solicitou aos fabricantes de dois softwares brasileiros gerenciadores de monitoramento que fornecessem material e informações para a pesquisa, mediante o compromisso de utilização exclusivamente acadêmica, ambas as respostas foram negativas.

A Dígitro[11], fabricante do sistema Guardião, enviou mensagem com o seguinte teor: "não podemos fornecer as informações solicitadas, em virtude de acordos de confidencialidade com nossos clientes de soluções destinadas à Segurança Pública"[12].

Já a Suntech[13], fabricante do sistema Vigia, respondeu que "todas as informações acerca do negócio e da empresa são confidenciais, por este motivo não poderemos auxiliá-lo nesta pesquisa"[14]. No caso deste último, no entanto, a empresa de telecomunicações Claro manteve disponível em seu *site*, por breve período, o manual de instruções do sistema Vigia[15], por meio do qual o autor teve acesso a alguns detalhes das ferramentas empregadas no monitoramento, de modo a poder ilustrar o capítulo.

Tais circunstâncias levarão a um limite no aprofundamento no segundo capítulo, tendo-se feito necessário recorrer a fontes não acadêmicas, como matérias jornalísticas. O autor presenciou e acompanhou os trabalhos de interceptação telefônica e telemática que se realizavam em dependências policiais, por período curtíssimo, até que fosse convidado a se retirar, de modo a impedir que pudesse tomar conhecimento de qualquer informação sigilosa, fosse a respeito dos alvos sob monitoramento, fosse sobre dados já coletados. Concederam-se, no entanto, após o concedente ter-se encarregado de inserir tarjas pretas sobre os dados sigilosos, cópias de telas do sistema, mostrando algumas das ferramentas utilizadas.

O autor, ademais, adquiriu um renomado software comercial de criptografia, de fabricação israelense, de modo a poder contar com um canal estreito de comunicação com o fabricante e, assim, compreender melhor o funcionamento de tal mecanismo e eventuais vulnerabilidades.

---

[11] DÍGITRO. Disponível em: <http://www.digitro.com.br/pt/>. Acesso em: 26 ago. 2013.

[12] PIAZERA, Isadora Bolduan. **RE: Esclarecimentos** [mensagem pessoal]. Mensagem recebida por <sidi@ffernandes.adv.br> em 14 out. 2013.

[13] SUNTECH GRUPO VERINT. Disponível em: <http://www.suntechintelligence.com/>. Acesso em: 26 ago. 2013.

[14] REIS, Flávia Michele Medeiros de Araújo. RE: Esclarecimentos [mensagem pessoal]. Mensagem recebida por <sidi@ffernandes.adv.br> em 14 out. 2013.

[15] SUNTECH VIGIA. Interception Achievement Suite. Manual do Usuário Vigia 3. Outubro/2011. Disponível em: <https://vigia.claro.com.br/VigiaDadosClient/custom/doc/Manual_VIGIA3_Consulta.pdf;jsessionid=17AC1571FB9CF8BA129C7D3821809BC9.tomcat1>. Acesso em: 14 out. 2013.

Para além disso, a época da pesquisa coincidiu com a eclosão do mencionado escândalo internacional protagonizado pelo ex-técnico da CIA Edward Snowden. Apesar da já narrada tentativa de censura imposta pelas agências de inteligência aos veículos *The Guardian*, *The New York Times* e *ProPublica*, estes declararam que se limitaram a omitir alguns fatos específicos, mas, ao final, decidiram por publicar a matéria, em razão do valor que vislumbraram num debate público sobre ações do governo capazes de enfraquecer as mais poderosas ferramentas de proteção à privacidade dos usuários da internet nos Estados Unidos e no mundo[16].

O nível de sigilo dos documentos revelados era tão expressivo, que estes continham advertências dirigidas aos próprios analistas das agências, como "*do not ask about or speculate on sources or methods underpinning Bullrun*" e "*there will be no 'need to know'*"[17].

Será graças à dita reportagem, bem como a escassos relatórios por meios dos quais órgãos de investigação e agências de inteligência acabam por divulgar alguns de seus êxitos mais populares, que o capítulo 2 se proporá a desfazer alguns dos mitos que envolvem os métodos modernos de investigação, trazendo-os à tona como realidade ou, ao menos, como algo mais perto da ideia de realidade do que da de ficção.

O capítulo 3, "A interceptação das comunicações telemáticas: diálogos de direito comparado", analisará esse método investigatório nos Estados Unidos da América, Inglaterra e Espanha, de modo a ampliar o campo de visão do autor sobre diferentes possibilidades de tratamento destinado às interceptações das comunicações telemáticas, viabilizando, assim, uma análise crítica mais rica e bem embasada.

No que se refere à escolha dos dois primeiros países, Estados Unidos e Inglaterra, ela se deveu ao potencial tecnológico de ambos, ao fato de terem sido o berço do desenvolvimento científico da maior parte das ferramentas comunicativas mais poderosas, à atuação tradicionalmente voraz de suas agências de inteligência e órgãos de investigação penal e – como não dizer – ao tratamento diferenciado que destinam à investigação de terrorismo desde o atentado às torres do *World Trade Center*, em 2001.

---

[16] BALL, James; BORGER, Julian; GREENWALD, Glenn. Revealed: how US and UK spy agencies defeat internet privacy and security. **The Guardian**. 06 set. 2013. Disponível em: <http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>. Acesso em: 29 set. 2013: "Intelligence officials asked the Guardian, New York Times and ProPublica not to publish this article, saying that it might prompt foreign targets to switch to new forms of encryption or communications that would be harder to collect or read. The three organisations removed some specific facts but decided to publish the story because of the value of a public debate about government actions that weaken the most powerful tools for protecting the privacy of internet users in the US and worldwide."

[17] Em tradução livre, respectivamente, "não perguntar ou especular sobre fontes ou métodos que sustentam o Projeto Bullrun" e "não haverá necessidade de saber".

Quanto à Espanha, a escolha do autor se deveu às peculiaridades de sua legislação sobre o tema, que é bastante detalhada, indicando tratar-se de um país com uma valiosa experiência a contribuir com o trabalho, o que também pode ser ilustrado com o fato de que o dia 28 de janeiro foi declarado pela Espanha o "dia de proteção de dados"[18]. E, é claro, uma razão adicional para a inclusão da Espanha na presente dissertação foi a intenção de diversificar as fontes, inserindo um país da Europa continental, formado, tal qual o Brasil, sob influências do *inquisitorial system*, o que se contrapõe aos dois primeiros países que, de origem anglo-saxônica, estão mais ligados ao *adversarial system*[19].

E, no capítulo 4, intitulado "A interceptação das comunicações telemáticas no Brasil", serão analisados os dispositivos constitucionais brasileiros de interesse do tema, os princípios e regras presentes no texto constitucional, suas restrições e âmbito de proteção, e a cláusula de exceção inserida na regra atinente à inviolabilidade do sigilo das comunicações (art. 5º, XII).

Feito isso, o quarto capítulo se ocupará da classificação probatória da medida de interceptação telemática, seus pressupostos, prazo, sujeitos legitimados a autorizá-la e a requerê-la, o incidente de inutilização de comunicações tidas por inúteis, o direito de acesso ao material captado, o tratamento da prova ilícita, da prova fortuitamente encontrada, da distinção de tratamento entre dados de tráfego e dados de conteúdo, da interceptação empregada preventivamente à ocorrência de um delito e das tecnologias de criptografia e sua regulamentação.

---

[18] El próximo 28 de enero se celebra "el Día de Protección de Datos... que tiene como objetivo principal impulsar el conocimiento entre los ciudadanos europeos de cuáles son sus derechos y responsabilidades en materia de protección de datos, de forma que puedan familiarizarse con un derecho fundamental, que pese a ser menos conocido, está presente en todas las faceta de sus vidas diarias." (ESPANHA. Agencia Española de Protección de Datos, Nota de Prensa. 19 jan. 2010. Disponível em: <https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2010/notas_prensa/common/enero/190110_np_previo_dia_europeo_2010.pdf>. Acesso em: 05 abr. 2013).

[19] Para evitar confusões terminológicas entre os binômios acusatório-inquisitório e *inquisitorial-adversarial*, traz-se a lição de Ada Pellegrini Grinover, que explica a distinção entre os modelos acusatório e inquisitório, afirmando que "no primeiro, as funções de acusar, defender e julgar são atribuídas a órgãos distintos, enquanto no segundo as funções estão reunidas e o inquisidor deve proceder espontaneamente". Mas esses dois conceitos, esclarece a Professora, "nada têm a ver com a iniciativa instrutória do juiz no processo penal", que está ligada, na realidade, com o chamado *adversarial system,* próprio do sistema anglo-saxão, em contraposição ao *inquisitorial system,* da Europa continental e dos países por ela influenciados. No *adversarial system*, há uma predominância das partes na determinação da marcha do processo e na produção das provas, enquanto, no *inquisitorial system,* ao revés, as mencionadas atividades recaem de preferência sobre o juiz, caracterizando um 'processo de desenvolvimento oficial'". (GRINOVER, Ada Pellegrini. A iniciativa instrutória do juiz no processo penal acusatório. In: **Revista Brasileira de Ciências Criminais**, São Paulo, ano 7, nº 27, jul-set 1999, Revista dos Tribunais, 1999. p. 71/72).

1 **INTIMIDADE, VIDA PRIVADA E INTERCEPTAÇÃO DAS COMUNICAÇÕES TELEMÁTICAS**

1.1 Intimidade e vida privada

Classificados por Canotilho (2000) como modalidades de direitos de personalidade, a intimidade e a vida privada pertencem ao grupo dos direitos[20] sobre a própria pessoa[21].

Baseado no trabalho de Henkel, Paulo José da Costa Jr. (2007) analisa a teoria dos círculos concêntricos, segundo a qual a vida privada se divide em várias esferas, de dimensões menores. A maior seria a da esfera privada *stricto senso* (*Privatsphäre*), na qual estariam todos os comportamentos e acontecimentos que o indivíduo não quer que se tornem de domínio público. Fora da esfera privada, estariam os processos, episódios e condutas de natureza pública, ao alcance da coletividade em geral, de um círculo indeterminado de pessoas. No bojo da esfera privada, estaria contida a esfera da intimidade (*Vertrauensphäre*) ou confidência (*Vertraulichkeitssphäre*), da qual participam somente as pessoas nas quais o indivíduo deposita certa confiança e com as quais mantém certa intimidade. Nela estão as conversações e acontecimentos íntimos. Dentro desta última, estaria a esfera do segredo (*Geheimsphäre*), que compreende aquela parcela da vida particular que é conservada em segredo pelo indivíduo, do qual compartilham uns poucos amigos, muito íntimos[22].

Segundo essa teoria, distingue-se, na esfera privada, o direito ao respeito à vida privada (*diritto al rispetto della vita privata* ou *diritto alla segretezza*) do direito à intimidade (*diritto alla riservatezza*). O primeiro consistiria no direito de impedir que a atividade de terceiro venha a conhecer ou descobrir as particularidades da vida privada alheia, direito de impedir que intrusos se intrometam em sua esfera particular. O segundo seria sucessivo ao direito à privacidade e consistiria no direito de a pessoa se defender da divulgação de notícias particulares, mas legitimamente conhecidas pelo divulgador[23].

---

[20] Ver distinção entre direitos e garantias no item 2.1.1, *infra*.
[21] CANOTILHO, José Joaquim Gomes. **Direito constitucional e teoria da Constituição**. 7ª ed. Coimbra: Almedina, 2000, p. 396.
[22] COSTA JR., Paulo José da. **O direito de estar só**: tutela penal da intimidade. 4ª ed. rev. e atual. São Paulo: Revista dos Tribunais, 2007, p. 29/30.
[23] Ibid., p. 25.

Noutras palavras, o direito à vida privada protegeria o indivíduo contra invasão ilegítima, enquanto o direito à intimidade tutelaria a vida privada contra a divulgação não autorizada de algo acessado licitamente[24].

O citado autor, no entanto, não vê razão para denominar diversamente as duas esferas privadas, preferindo chamar ambas de direito à intimidade, pois pouco importaria se se trataria de preservá-la ou de mantê-la. Afinal, na expressão direito à intimidade, há dois interesses, na não agressão e na não divulgação, mas o direito é o mesmo[25].

Intimidade é a faculdade que o indivíduo tem de se isolar, conforme o seu caráter, a sua tendência ou a sua disposição de espírito, independentemente das solicitações a que esteja exposto[26].

O isolamento é ingrediente para o desenvolvimento sadio da personalidade, de seus valores físicos e psíquicos[27]. Isolar-se é uma necessidade humana, retratada, aliás, em passagem da clássica obra "Recordação da casa dos mortos", de Dostoiévski (1949), em que relata seu período de reclusão em um presídio da Sibéria:

> Haverá por exemplo tormento maior do que não poder ficar sozinho – um momento ao menos – e isso durante dez anos? No trabalho: a escolta, no presídio: a companhia de mais de duzentos detentos; e: nunca, uma só vez, a solidão! Ter que ser assim, irrevogavelmente![28]

A intimidade dá ao indivíduo o arbítrio de querer ou não revelar aspectos de sua vida, permitindo-lhe excluir do conhecimento de terceiros aquilo que guarda relação estreita ou estreitíssima com si próprio e que em nada o engrandece ou com ele contribui quando apreendido pelo universo exterior, servindo apenas a dessedentar a curiosidade alheia[29].

Quanto à distinção entre intimidade e privacidade, a maioria dos doutrinadores que se propuseram a estabelecê-la concorda em situá-la na diferença de níveis de concentração de uma mesma substância.

Nesse sentido, entre ambas haveria uma relação de gênero (privacidade) e espécie (intimidade), na medida em que o íntimo é mais do que o privado, sendo o conceito de vida

---

[24] Ibid., p. 26.
[25] Ibid., p. 27/28.
[26] PEREIRA, Caio Mario da Silva. **Direito civil**: alguns aspectos da sua evolução. Rio de Janeiro: Forense, 2001, p. 29.
[27] JABUR, Gilberto Haddad. **Liberdade de pensamento e direito à vida privada**: conflitos entre direitos da personalidade. São Paulo: Revista dos Tribunais, 2000, p. 253.
[28] DOSTOIEVSKI, Fedor M. **Recordação da casa dos mortos**. Tradução Geraldo Vieira. São Paulo: Saraiva, 1949, p. 15.
[29] JABUR, 2000, p. 253.

privada, enfim, mais amplo do que o de intimidade[30]. A privacidade pode ser limitada, abarcando tudo aquilo que, simplesmente, não se quer que esteja acessível ao conhecimento dos demais. Dentro dela, da vida privada, estará um núcleo que se protege com mais força, um núcleo considerado essencial à configuração subjetiva do indivíduo, a intimidade[31].

A intimidade seria o mais exclusivo dos direitos no âmbito da privacidade, havendo entre eles, portanto, "uma certa gradação nos direitos da privacidade"[32].

Sob outro ponto de vista, a privacidade seria composta de valores que, apesar de próprios ou exclusivos, seriam sempre exercidos perante os outros, enquanto que a intimidade seria o âmbito exclusivo que alguém reserva para si, sem nenhuma repercussão social, nem mesmo ao alcance da vida privada[33].

Não nos parecendo relevante a demarcação do exato limite que separa a privacidade da intimidade, ao menos para o que se propõe o presente trabalho, temos que, embora com diferentes níveis hierárquicos, tanto uma quanto outra interessam ao estudo da interceptação das comunicações telemáticas, tendo em vista que a quebra do sigilo das comunicações de um indivíduo, cujo teor captado será, naturalmente, imprevisível e incontrolável, terá o potencial de revelar, desde a informação mais desimportante na vida do investigado, cuja divulgação sequer lhe traria qualquer incômodo ou constrangimento, até seu mais caro e íntimo segredo.

---

[30] BASTERRA, Marcela I. Prueba y médios de comunicación: la cuestión constitucional. In: ARAZI, Roland (Org.). **Prueba ilícita y prueba científica**. Santa Fe, Argentina: Rubinzal-Culzoni Editores, 2008, p. 262.

[31] BASTERRA, 2008, p. 262.

[32] FERRAZ JR., Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito da Universidade de São Paulo**, São Paulo, v. 88, p. 439/459, jan./dez. 1993, p. 442. Para Gilmar Ferreira Mendes, Inocêncio Coelho e Paulo Gonet, o direito à privacidade tem por objeto os comportamentos e acontecimentos atinentes aos relacionamentos pessoais em geral e às relações comerciais e profissionais que o indivíduo não deseja que se tornem públicas, ao passo que o objeto da intimidade seriam as conversações e os episódios ainda mais íntimos, envolvendo relações familiares e amizades mais próximas (MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**. 2ª ed. rev. e atual. São Paulo: Saraiva, 2008, p. 377).

[33] Para Tércio Sampaio Ferraz, no âmbito da privacidade, sempre exercida perante os outros, estariam o direito ao nome, à imagem, à reputação, as formas de convivência que, embora exclusivas, teriam na comunicação um elemento inevitável, como a vida na família, no trabalho, no lazer em comum, um viver, enfim, entre os outros, e que demarca justamente a individualidade em face desses outros. Já na intimidade, âmbito exclusivo que alguém reserva para si, sem nenhuma repercussão social, estariam o diário íntimo, o segredo sob juramento, as próprias convicções, as situações indevassáveis de pudor pessoal e o segredo íntimo cuja mínima publicidade constrange (FERRAZ JR., 1993, p. 442/443). Para René Ariel Dotti, ao contrário, a intimidade se projetaria também no exterior. O autor a define como um sentimento, um estado da alma, que existe nos ambientes interiores, mas que se projeta também no exterior, para ser possível viver a liberdade de amar, pensar, sorrir, chorar, rezar, enfim viver a própria vida e morrer a própria morte, ou seja, é uma das liberdades fundamentais do corpo, da mente e do espírito (DOTTI, René Ariel. A liberdade e o direito à intimidade. In: **Revista de Informação Legislativa**, Brasília, ano 17, nº 66, p. 125/152, abr./jun. 1980, p. 130). Edson Ferreira da Silva, sem preocupação em demarcar uma distinção bem definida, sustenta que a intimidade compreende o poder jurídico do indivíduo de subtrair do conhecimento alheio e de impedir qualquer forma de divulgação de aspectos de sua vida privada, que, segundo um senso comum, variável em cada época e lugar, interessaria manter sob reserva (SILVA, Edson Ferreira da. **Direito à intimidade**: de acordo com a doutrina, o direito comparado, a Constituição de 1988 e o Código Civil de 2002. 2ª ed. São Paulo: J. de Oliveira, 2003, p. 51).

1.2 Intimidade e vida privada como direitos fundamentais

Antes de tratar da intimidade e da vida privada como direitos fundamentais, importa distinguir direitos e garantias.

Rui Barbosa (1955) diferenciou direitos de garantias afirmando que estas últimas são "postas pela Constituição aos direitos especiais do indivíduo", integrando o "sistema de proteção organizado pelos autores da nossa lei fundamental em segurança da pessoa humana, da vida humana, da liberdade humana", ao abrigo do qual "se acha a nossa personalidade, a nossa humanidade, a nossa existência mesma, contra os impulsos dos governos violentos."[34]

Canotilho (2000) afirma que as clássicas garantias são também direitos, embora seja comum se salientar o caráter instrumental das garantias na proteção dos direitos. Seria garantia o direito dos cidadãos de exigir dos poderes públicos a proteção dos seus direitos e o reconhecimento dos meios processuais adequados a essa finalidade, o que exemplificou com o direito de acesso aos tribunais para a defesa de direitos, princípios do *nullum crimen sine lege* e *nulla poena sine crimen*, direito de *habeas corpus* e princípio *non bis in idem*[35].

A diferença, segundo Celso Ribeiro Bastos (2010), repousa na circunstância de que as garantias não resguardam bens da vida propriamente ditos, tais como a liberdade, a propriedade e a segurança, mas fornecem instrumentos jurídicos ao indivíduo, especialmente fortes e rápidos, para garantir os direitos individuais[36].

Entendemos, portanto, que intimidade e vida privada, como expressões autônomas, desacompanhadas de dispositivos prevendo instrumentos para a sua salvaguarda, constituem direitos, e não garantias[37].

---

[34] BARBOSA, Rui. Discursos parlamentares: sessão de 05 de agosto de 1905 do Senado Federal. In: NERY, Fernando (Org.). **Obras completas de Rui Barbosa**, v. XXXII, tomo I, Rio de Janeiro: Ministério da Educação e Cultura, 1955, p. 23.

[35] CANOTILHO, 2000, p. 396.

[36] BASTOS, Celso Ribeiro. **Curso de direito constitucional**. 22ª ed. rev. e atual. por Samantha Meyer-Pflug. São Paulo: Malheiros, 2010, p. 248.

[37] Na Constituição brasileira, que será abordada no item 4.1, o inciso X do artigo 5º estabelece a inviolabilidade da intimidade e da vida privada, dando a cada indivíduo o direito de obstar a intromissão de estranhos na sua vida privada e familiar, assim como de lhes impedir o acesso a informações sobre a privacidade de cada um, e também de impedir que sejam divulgadas informações sobre esta área da manifestação existencial do ser humano. Desdobramento desta norma se encontra inscrito no inciso XII do mesmo artigo 5º, que, através da afirmação da inviolabilidade da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, também visam a preservar as coisas íntimas e privadas (BASTOS, 2010, p. 305). Diante disso, entendemos que a intimidade e a vida privada, bem como a inviolabilidade do sigilo das comunicações figuram na Constituição brasileira como direitos, e não como garantias, pois os dispositivos que as consagram não preveem instrumentos ou meios processuais adequados à sua tutela, mas apenas as afirmam. Apesar de concordar com essa diferenciação, Mendes, Coelho e Branco trazem interessante ressalva. Dizem que as normas que protegem um objeto imediato, como a vida, a honra e a liberdade física seriam direitos, enquanto as normas

Os direitos fundamentais, hoje inscritos em constituições e diplomas internacionais, são decorrência de evolução histórica que é objeto de estudos profundos em direito constitucional, ciência cujo significado atual decorre da afirmação de que os direitos fundamentais constituem o núcleo da proteção da dignidade da pessoa e de que as normas que assegurarão esses valores devem estar inseridas num documento jurídico chamado constituição[38]. Um marco histórico relevante para a trajetória desta evolução foi o cristianismo, com o dogma de que o homem possui a imagem de Deus[39], o que eleva o valor da espécie humana[40].

Depois, o contratualismo dos séculos XVII e XVIII deu base teórica a uma prevalência do indivíduo sobre o poder político, com afirmação de que determinados direitos, por resultarem da condição humana, são anteriores ao próprio Estado, que passa a ser visto como instituição voltada para garantir aos cidadãos os direitos básicos[41]. Em 1776, essas ideias são positivadas na Declaração de Direitos da Virginia[42], após o que, em 1789, na Declaração Francesa e, em 1791, na *Bill of Rights*, que inseriu na Constituição dos Estados Unidos da América, através de emendas, os direitos tidos como inerentes ao homem. São os chamados direitos fundamentais de primeira geração[43].

---

que protegem esses direitos indiretamente, limitando, por vezes procedimentalmente, o exercício do poder, seriam os direitos-garantias, as garantias fundamentais, que asseguram ao indivíduo a possibilidade de exigir dos Poderes Públicos o respeito ao direito que instrumentalizam. Ressalvam que, embora a fronteira entre um e outra nem sempre se apresente límpida, não há nisso maior importância prática, uma vez que a ordem constitucional brasileira teria conferido tratamento unívoco aos direitos e às garantias fundamentais (MENDES, COELHO; BRANCO, 2008, p. 268).

[38] MENDES; COELHO; BRANCO, 2008, p. 231.

[39] Gênesis 1:25-27: "E fez Deus as feras da terra conforme a sua espécie, e o gado conforme a sua espécie, e todo o réptil da terra conforme a sua espécie; e viu Deus que era bom. E disse Deus: Façamos o homem à nossa imagem, conforme a nossa semelhança; e domine sobre os peixes do mar, e sobre as aves dos céus, e sobre o gado, e sobre toda a terra, e sobre todo o réptil que se move sobre a terra. E criou Deus o homem à sua imagem: à imagem de Deus o criou; homem e mulher os criou."

[40] MENDES; COELHO; BRANCO, 2008, p. 232.

[41] Ibid., p. 232.

[42] The Virginia Declaration of Rights: "Section 1. That all men are by nature equally free and independent and have certain inherent rights, of which, when they enter into a state of society, they cannot, by any compact, deprive or divest their posterity; namely, the enjoyment of life and liberty, with the means of acquiring and possessing property, and pursuing and obtaining happiness and safety. Section 2. That all power is vested in, and consequently derived from, the people; that magistrates are their trustees and servants and at all times amenable to them."

[43] Explica-se a nomenclatura *direitos de primeira geração* com o fato de que foram eles, com as Revoluções Americana e Francesa, os primeiros a serem positivados. Os de segunda geração são os chamados direitos sociais, a exemplo do direito de greve e de sindicalização. Já os de terceira geração são os de titularidade difusa ou coletiva, como o direito à paz, ao desenvolvimento, à qualidade do meio ambiente e à conservação do patrimônio histórico e cultural (MENDES; COELHO; BRANCO, 2008, p. 233/234).

A expectativa de um direito à intimidade surge com o nascimento da burguesia como classe social e com os núcleos urbanos, cujo desenvolvimento se viabilizou com a melhora das condições sociais e econômicas[44].

Na incerteza quanto ao primeiro precedente judicial sobre a proteção à intimidade, a doutrina costuma se referir ao caso em que a irmã de uma famosa artista francesa pedira a dois pintores que a desenhassem em seu leito mortuário, expondo, em seguida, a imagem publicamente e colocando-a à venda. O caso foi julgado pelo Tribunal Civil do Sena, em 16 de junho de 1858, que determinou a apreensão do desenho e de suas várias provas fotográficas[45].

Além deste precedente, menciona-se um artigo doutrinário, publicado na *Harvard Law Review*[46], em 1890, pelos advogados norte-americanos Samuel Dennis Warren e Louis Dembitz Brandeis, intitulado *The right to privacy*, em que, incomodados com as constantes publicações da imprensa expondo intimidades sobre a família de um deles, trataram da necessidade de se proteger a privacidade das pessoas, vindo, depois, a levar o caso à Suprema Corte dos Estados Unidos. A tese, apesar de rejeitada por quatro votos a três, obteve a simpatia da opinião pública, que se posicionou ao lado dos juízes vencidos, levando a Corte a, mais tarde, vir a reconhecer o direito à intimidade[47].

1.3 A proteção à vida privada e à intimidade no cenário internacional

A proteção à vida privada e à intimidade é hoje reconhecida internacionalmente, estando tutelada nas principais cartas internacionais de direitos humanos. A Declaração Universal dos Direitos Humanos (DUDH), em seu artigo 12, assegura que "ninguém será

---

[44] MORI, Michele Keiko. **Direito à intimidade versus informática**. Curitiba: Juruá, 2001, p. 13.

[45] COSTA JR., 2007, p. 11/12: Diz o autor que da decisão constou que, por maior que seja uma artista, por histórico que seja um grande homem, tem sua vida privada distinta da pública, seu lar separado da cena e do fórum. Podem desejam morrer na obscuridade, quando ou porque viveram no triunfo (*Jurisprudence français en matière de droit civil, Rev. trimestrielle de droit civil*, jan./mar. 1971, p. 111).

[46] WARREN, Samuel Dennis; BRANDEIS, Louis Dembitz. The right to privacy. **Harvard Law Review**, v. IV, nº 5, 15.12.1890, Disponível em: <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>. Acesso em: 05 mai. 2012.

[47] COSTA JR., 2007, p. 12/13.

sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques à sua honra e reputação"[48].

O artigo 11(2) da Convenção Americana sobre Direitos Humanos (CADH)[49] dispõe que "Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação."

Também o artigo 8º da Convenção Europeia para a Proteção aos Direitos Humanos (CEDH) dispõe que "qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência", acrescentando que "não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar econômico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros."

Como pontuaremos no item 4.1.1, dos direitos à intimidade e à privacidade advém uma proteção ao sigilo das comunicações, que algumas constituições preveem expressamente. Na Constituição brasileira, por exemplo, desdobramento do princípio protetor da inviolabilidade da intimidade e da vida privada (art. 5º, X) se encontra na regra de proteção à inviolabilidade do sigilo das comunicações (art. 5º, XII)[50].

A jurisprudência do Tribunal Europeu de Direitos Humanos (TEDH) é no sentido de que a expressão "prevista na lei", do artigo 8º(2) da CEDH[51], exige que eventual medida que afaste o sigilo das comunicações esteja expressamente prevista na lei interna do Estado-Parte; que se trate de norma acessível a todos, mediante os meios de publicação; e que tal norma preveja, com clareza e precisão, as condições pelas quais os poderes públicos estão autorizados a adotar a medida, dando ao indivíduo previsibilidade das suas consequências.

Quanto às demais exigências do mesmo artigo 8º, há precedentes daquela Corte reconhecendo a legitimidade da restrição ao sigilo de comunicações para a proteção da

---

[48] Adotada e proclamada pela resolução 217 A (III), da Assembleia Geral das Nações Unidas em 10 de dezembro de 1948.
[49] Promulgada no Brasil através do Decreto nº 678/92.
[50] BASTOS, 2010, p. 305.
[51] CEDH: "Art. 8º (Direito ao respeito pela vida privada e familiar) 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infracções penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros."

segurança nacional[52], para a defesa da ordem[53], para o bem estar econômico do país[54], para a prevenção do crime[55], para a proteção da saúde[56] e para a proteção à moral[57].

Na percepção de Benjamim Rodrigues (2009), o entendimento do TEDH é o de admitir a restrição ao sigilo de comunicações como *ultima ratio*, sendo a regra a

---

[52] "In the light of these considerations and of the detailed examination of the contested legislation, the Court concludes that the German legislature was justified to consider the interference resulting from that legislation with the exercise of the right guaranteed by Article 8 para. 1 (art. 8-1) as being necessary in a democratic society in the interests of national security and for the prevention of disorder or crime (Article 8 para. 2) (art. 8-2). Accordingly, the Court finds no breach of Article 8 (art. 8) of the Convention." (TRIBUNAL EUROPEU DE DIREITOS HUMANOS. Caso Klass et al. vs. Germany. Disponível em: <http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=klass&sessionid=90267778&skin=hudoc-en>. Acesso em: 07 abr. 2012).

[53] "Although the applicant argued that the interference did not pursue a legitimate aim (see paragraph 39 above) the Court sees no reason to doubt that the letters were opened for "the prevention of disorder or crime" within the meaning of Article 8 para. 2 (art. 8-2)" (TRIBUNAL EUROPEU DE DIREITOS HUMANOS. Caso Campbell vs. The United Kingdom. Disponível em: <http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=campbell&sessionid=90267778&skin=hudoc-en>. Acesso em: 01 abr. 2012).

[54] "The relevant legislation was thus designed to promote the economic well-being of the island. The Court does not find it to be established that the legislation pursued any other purpose" (TRIBUNAL EUROPEU DE DIREITOS HUMANOS. Caso Gillow vs. The United Kingdom. Disponível em: <http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=gillow&sessionid=90267778&skin=hudoc-en>. Acesso em: 03 abr. 2012).

[55] "The Government and the Commission considered that the interferences in question were in the interests of 'the economic well-being of the country' and 'the prevention of crime'." (TRIBUNAL EUROPEU DE DIREITOS HUMANOS. Caso Funke vs. France. Disponível em: <http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=funke&sessionid=90267778&skin=hudoc-en>. Acesso em: 03 abr. 2012).

[56] "64. The applicants submitted that, of the aims listed in paragraph 2 of Article 8 (art. 8-2), only the 'protection of health or morals' could have justified the decision to take the children into care, but that their health or morals were not in fact endangered when it was adopted. The Commission, on the other hand, considered that the decisions concerning the care and the placement of the children were taken in their interests and had the legitimate aims of protecting health or morals and protecting the 'rights and freedoms of others'. 65. In the Court's view, the relevant Swedish legislation is clearly designed to protect children and there is nothing to suggest that it was applied in the present case for any other purpose. The interferences in question - intended as they were to safeguard the development of Stefan, Helena and Thomas - therefore had, for the purposes of paragraph 2 of Article 8 (art. 8-2), the legitimate aims attributed to them by the Commission." (TRIBUNAL EUROPEU DE DIREITOS HUMANOS. Caso Olsson vs. Sweden. Disponível em: <http://cmiskp.echr.coe.int/tkp197/view.asp?item=2&portal=hbkm&action=html&highlight=olsson&sessionid=90267778&skin=hudoc-en>. Acesso em: 07 abr. 2012).

[57] "62. In the opinion of the Commission, the interference complained of by the applicant can, in so far as he is prevented from having sexual relations with young males under 21 years of age, be justified as necessary for the protection of the rights of others (see especially paragraphs 105 and 116 of the report). This conclusion was accepted and adopted by the Government, but disputed by the applicant who submitted that the age of consent for male homosexual relations should be the same as that for heterosexual and female homosexual relations that is, 17 years under current Northern Ireland law (see paragraph 15 above). The Court has already acknowledged the legitimate necessity in a democratic society for some degree of control over homosexual conduct notably in order to provide safeguards against the exploitation and corruption of those who are specially vulnerable by reason, for example, of their youth (see paragraph 49 above). However, it falls in the first instance to the national authorities to decide on the appropriate safeguards of this kind required for the defence of morals in their society and, in particular, to fix the age under which young people should have the protection of the criminal law (see paragraph 52 above)." (TRIBUNAL EUROPEU DE DIREITOS HUMANOS. Caso Dudgeon vs. The United Kingdom. Disponível em: <http://cmiskp.echr.coe.int/tkp197/view.asp?item=2&portal=hbkm&action=html&highlight=dudgeon&sessionid=90267778&skin=hudoc-en>. Acesso em: 01 abr. 2012).

inviolabilidade do sigilo e a exceção seu afastamento, admissível quando não existirem outros meios menos danosos ou lesivos aos direitos fundamentais[58].

Há um precedente referente, não à interceptação telemática, mas à telefônica, o que, no entanto, demonstra o entendimento da Corte sobre questão que lhe seria aplicável. Trata-se do caso Kopp vs. Suíça, em que o escritório do advogado Kopp, o reclamante, teve todas as suas linhas telefônicas monitoradas entre novembro e dezembro de 1989. O TEDH entendeu que o Estado Suíço violou o artigo 8º (2) da Convenção e que ao reclamante não restou assegurado o mínimo de proteção de que se deve dispor numa sociedade democrática, porque a legislação interna não seria dotada de precisão e clareza quanto à existência de normas detalhadas para interceptação e porque, mesmo havendo previsão interna de que a inviolabilidade absoluta das comunicações do advogado só seria aplicável às conversas que tratassem de temas ligados à advocacia, a lei suíça não dispunha claramente como, sob quais condições e a quem caberia distinguir entre assuntos que fossem ligados à advocacia e os que lhe fossem estranhos, verificando-se, portanto, que a lei suíça não indicava, com clareza, a forma pela qual as autoridades deveriam exercer sua discricionariedade sobre a matéria[59].

No caso Calogero Diana vs. Itália, o reclamante, condenado à prisão perpétua por atividades terroristas, questionava a violação de todas as correspondências que mantinha com o mundo exterior, inclusive com seu advogado. O pedido do condenado para que a medida cessasse foi negado, tendo em vista a gravidade do crime, a sua não cooperação com os

---

[58] RODRIGUES, 2009, p. 125.

[59] "Secondly, tapping and other forms of interception of telephone conversations constitute a serious interference with private life and correspondence and must accordingly be based on a "law" that is particularly precise. It is essential to have clear, detailed rules on the subject, especially as the technology available for use is continually becoming more sophisticated (see the above-mentioned Kruslin and Huvig judgments, p. 23, § 33, and p. 55, § 32, respectively). In that connection, the Court by no means seeks to minimise the value of some of the safeguards built into the law, such as the requirement at the relevant stage of the proceedings that the prosecuting authorities' telephone-tapping order must be approved by the President of the Indictment Division (see paragraphs 18 and 35 above), who is an independent judge, or the fact that the applicant was officially informed that his telephone calls had been intercepted (see paragraph 25 above). 73. However, the Court discerns a contradiction between the clear text of legislation which protects legal professional privilege when a lawyer is being monitored as a third party and the practice followed in the present case. Even though the case-law has established the principle, which is moreover generally accepted, that legal professional privilege covers only the relationship between a lawyer and his clients, the law does not clearly state how, under what conditions and by whom the distinction is to be drawn between matters specifically connected with a lawyer's work under instructions from a party to proceedings and those relating to activity other than that of counsel. 74. Above all, in practice, it is, to say the least, astonishing that this task should be assigned to an official of the Post Office's legal department, who is a member of the executive, without supervision by an independent judge, especially in this sensitive area of the confidential relations between a lawyer and his clients, which directly concern the rights of the defence. 75. In short, Swiss law, whether written or unwritten, does not indicate with sufficient clarity the scope and manner of exercise of the authorities' discretion in the matter. Consequently, Mr Kopp, as a lawyer, did not enjoy the minimum degree of protection required by the rule of law in a democratic society. There has therefore been a breach of Article 8." (TRIBUNAL EUROPEU DE DIREITOS HUMANOS. Caso Kopp vs. Suíça. Disponível em: <http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=kopp&sessionid=90267778&skin=hudoc-en>. Acesso em: 01 Abr. 2012).

funcionários da prisão, a sua oposição às instituições do Estado e o fato de que a confidencialidade da relação cliente-advogado estaria preservada nas entrevistas pessoais que se realizavam na prisão. O Tribunal reconheceu violação ao artigo 8º porque a lei interna deixaria às autoridades uma margem excessiva de discricionariedade, limitando-se a indicar a categoria de pessoas cuja correspondência poderia ser submetida a controle e o juiz competente, sem dispor sobre a duração da medida ou sobre os motivos que poderiam justificá-la[60].

No já citado caso Klass vs. Alemanha, o TEDH reconheceu que o termo "correspondência", presente no artigo 8(1) da Convenção Europeia, se estende a outras formas de comunicação privada, no caso a telefônica, que, no entanto, não é expressamente protegida naquela Convenção[61].

A Corte IDH possui também diversos precedentes em que foram apreciadas questões atinentes à intimidade e à vida privada.

No caso Atala Riffo y Niñas vs. Chile, a Corte decidiu que o artigo 11 da Convenção Americana, intitulado "Proteção à honra e à dignidade", tutela a vida privada, que seria um conceito amplo no qual estariam compreendidos, entre outros, a vida sexual e o direito de estabelecer e desenvolver relações com outros seres humanos, incluindo a forma como o indivíduo vê a si próprio e o quanto decide divulgar aos outros. Ainda nesse precedente, a Corte afirmou que o direito à vida privada não é absoluto, podendo ser restringido pelo Estado, desde que as ingerências não sejam abusivas ou arbitrárias e desde que as medidas invasivas estejam previstas em lei e que obedeçam aos requisitos da adequação, necessidade e proporcionalidade[62].

---

[60] TRIBUNAL EUROPEU DE DIREITOS HUMANOS. Caso Calogero Diana vs. Itália. Disponível em: <http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=calogero&sessionid=90267778&skin=hudoc-en>. Acesso em: 01 abr. 2012.

[61] "41. The first matter to be decided is whether and, if so, in what respect the contested legislation, in permitting the above-mentioned measures of surveillance, constitutes an interference with the exercise of the right guaranteed to the applicants under Article 8 para. 1 (art. 8-1). Although telephone conversations are not expressly mentioned in paragraph 1 of Article 8 (art. 8-1), the Court considers, as did the Commission, that such conversations are covered by the notions of "private life" and "correspondence" referred to by this provision." (TRIBUNAL EUROPEU DE DIREITOS HUMANOS. Caso Klass et al. vs. Germany. Disponível em: <http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57510>. Acesso em: 30 Jun. 2012).

[62] "El Tribunal ha establecido en su jurisprudencia que el derecho a la vida privada no es un derecho absoluto y, por lo tanto, puede ser restringido por los Estados siempre que las injerencias no sean abusivas o arbitrarias. Por ello, las mismas deben estar previstas en ley, perseguir un fin legítimo y cumplir con los requisitos de idoneidad, necesidad y proporcionalidad, es decir, deben ser necesarias en una sociedad democrática. … Además, el Tribunal ha precisado, respecto al artículo 11 de la Convención Americana, que, si bien esa norma se titula "Protección de la Honra y de la Dignidad", su contenido incluye, entre otros, la protección de la vida privada[62]. La vida privada es un concepto amplio que no es susceptible de definiciones exhaustivas y comprende, entre otros ámbitos protegidos, la vida sexual y el derecho a establecer y desarrollar relaciones con otros seres humanos[62]. Es decir, la vida privada incluye la forma en que el individuo se ve a sí mismo y cómo y cuándo decide proyectar a los demás." (CORTE INTERAMERICANA DE DIREITOS HUMANOS. Caso Atala Riffo y

No caso Escher e outros vs. Brasil, a Corte reconheceu que as comunicações telefônicas, ainda que não mencionadas expressamente no artigo 11 da Convenção, estão incluídas no âmbito de proteção da vida privada, que deve tutelar também o indivíduo tanto contra as operações técnicas dirigidas a registrar o conteúdo das comunicações, como contra o acesso a outros elementos do processo comunicativo, como informações atinentes ao destino e origem das chamadas, a identidade dos interlocutores, a frequência, hora e duração das chamadas ou outros aspectos que podem ser constatados sem necessidade de captar o conteúdo da conversa realizada. Reiterou-se, ainda, o entendimento de que a medida de interceptação de comunicações precisa "*a) estar prevista em lei, b) perseguir um fim legítimo e c) ser idônea, necessária e proporcional*", elementos sem os quais haveria ferimento à Convenção. Ao final, a Corte vislumbrou ferimento à Convenção porque identificou excesso de prazo na interceptação, em afronta à legislação interna, além de divulgação do material gravado através da imprensa, circunstâncias que afastaram a medida estatal das determinações da lei[63].

Niñas vs. Chile. Disponível em: <http://www.corteidh.or.cr/docs/casos/articulos/seriec_239_esp.doc>. Acesso em: 14 jul. 2012).

[63] "...ainda que as conversações telefônicas não se encontrem expressamente previstas no artigo 11 da Convenção, trata-se de uma forma de comunicação incluída no âmbito de proteção da vida privada ... O artigo 11 protege as conversas realizadas através das linhas telefônicas instaladas nas residências particulares ou nos escritórios, seja seu conteúdo relacionado a assuntos privados do interlocutor, seja com o negócio ou a atividade profissional que desenvolva. Desse modo, o artigo 11 aplica-se às conversas telefônicas independentemente do conteúdo destas, inclusive, pode compreender tanto as operações técnicas dirigidas a registrar esse conteúdo, mediante sua gravação e escuta, como qualquer outro elemento do processo comunicativo, como, por exemplo, o destino das chamadas que saem ou a origem daquelas que ingressam; a identidade dos interlocutores; a frequência, hora e duração das chamadas; ou aspectos que podem ser constatados sem necessidade de registrar o conteúdo da chamada através da gravação das conversas. Finalmente, a proteção à vida privada se concretiza com o direito a que sujeitos distintos dos interlocutores não conheçam ilicitamente o conteúdo das conversas telefônicas ou de outros aspectos, como os já elencados, próprios do processo de comunicação. ... Conforme já se afirmou (supra par. 116), para que esteja conforme com a Convenção Americana uma ingerência deve cumprir com os seguintes requisitos: a) estar prevista em lei, b) perseguir um fim legítimo e c) ser idônea, necessária e proporcional. Em consequência, a falta de algum desses requisitos implica que a ingerência seja contrária à Convenção. ... 146. A Corte conclui que as interceptações e gravações das conversas telefônicas objeto deste caso não observaram os artigos 1º, 2º, 3º, 4º, 5º, 6º e 8º da Lei No. 9.296/96 e, por isso, não estavam fundadas em lei. Em consequência, ao descumprir o requisito de legalidade, não resulta necessário continuar com a análise quanto à finalidade e à necessidade da interceptação. Com base no anterior, a Corte conclui que o Estado violou o direito à vida privada, reconhecido no artigo 11 da Convenção Americana, em relação com a obrigação consagrada no artigo 1.1 do mesmo tratado em prejuízo de Arlei José Escher, Dalton Luciano de Vargas, Delfino José Becker, Pedro Alves Cabral e Celso Aghinoni. ... 150. A Corte observa que trechos das gravações obtidas por meio das interceptações telefônicas foram exibidos em 7 de junho de 1999 no noticiário Jornal Nacional (supra par. 94). Não existiu uma investigação pela entrega à rede de televisão do material probatório que se encontrava sob custódia estatal e protegido pelo segredo de justiça, e que serviu de base para a reportagem mencionada. Ante a ausência de investigação por parte do Estado para determinar o ocorrido, a informação ilegitimamente entregue e os agentes estatais responsáveis (infra par. 205), não se pode determinar com exatidão o conteúdo do material levado ao conhecimento de terceiros, nesse caso, das pessoas que decidiram publicar e que elaboraram tal notícia no canal de televisão. ... a Corte considera que manter sigilo quanto às conversas telefônicas interceptadas durante uma investigação penal é um dever estatal: a) necessário para proteger a vida privada das pessoas sujeitas a uma medida de tal natureza; b) pertinente para os efeitos da própria investigação; e c) fundamental para a adequada administração da justiça. No presente caso, tratava-se de informação que deveria

Mais adiante, no capítulo 4, os precedentes reunidos no presente capítulo subsidiarão a análise crítica pretendida com o trabalho.

1.4 Eficiência e garantismo e o princípio da proporcionalidade

O binômio eficiência e garantismo constitui uma importante premissa para a análise à qual se propõe o presente trabalho. As concepções sobre ele foram pontuadas por Antonio Scarance Fernandes em três célebres publicações[64].

A primeira concepção é a de que tanto o direito à segurança quanto à liberdade constituem interesses relevantes[65], razão pela qual os indivíduos têm direito a que o Estado atue de modo a estruturar órgãos e criar procedimentos que, ao mesmo tempo, lhes forneçam segurança e lhes garantam a liberdade[66].

Não existe, no entanto, um antagonismo entre eficiência e garantismo, entendendo-se ser eficiente o processo que, além de permitir uma adequada persecução penal, também possibilite a incidência real das normas de garantia[67].

Ada Pellegrini Grinover (1996) reconhece que a exigência de eficácia do processo encontrará sempre barreiras intransponíveis nas garantias das partes e da defesa, pois não poderá fazer-se com sacrifício do juiz natural, do contraditório, do direito de defesa, da presunção de inocência, da motivação, da publicidade e de todas as demais garantias hoje conquistadas pelo processo constitucional[68]. No entanto, também não vê incompatibilidade

---

permanecer apenas em conhecimento de um reduzido número de funcionários policiais e judiciais e o Estado falhou em sua obrigação de mantê-la sob o devido resguardo. ... o Estado violou os direitos à vida privada, à honra e à reputação, reconhecidos nos artigos 11.1 e 11.2 da Convenção Americana." (CORTE INTERAMERICANA DE DIREITOS HUMANOS. Caso Escher e outros vs. Brasil. Disponível em: <http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf>. Acesso em 14 jul. 2012).

[64] FERNANDES, Antonio Scarance. O equilíbrio na repressão ao crime organizado. In: _____; ALMEIDA, José Raul Gavião; MORAES, Maurício Zanoide de (Coord.). **Crime organizado**: aspectos processuais. São Paulo: Revista dos Tribunais, 2009, p. 9/27; _____. Reflexões sobre as noções de eficiência e de garantismo no processo penal. In: _____; ALMEIDA, José Raul Gavião; MORAES, Maurício Zanoide de (Coord.). **Sigilo no processo penal**. São Paulo: Revista dos Tribunais, 2008, p. 9/28; e _____. O equilíbrio entre a eficiência e o garantismo e o crime organizado. In: **Revista Brasileira de Ciências Criminais**, São Paulo, v. 16, n. 70, p. 226/266, jan./fev. 2008.

[65] No Brasil, ambos estão inseridos no *caput* do art. 5º da CF.

[66] Id., 2008b, p. 9.

[67] Id., 2009, p. 9/10.

[68] GRINOVER, Ada Pellegrini. **Procedimentos sumários em matéria penal**: o processo em evolução. Rio de Janeiro: Forense Universitária, 1996, p. 278.

entre garantismo e eficiência, que diz constituírem os valores fundamentais do novo processo latino-americano[69].

A segunda concepção é a de que deve haver um equilíbrio adequado, no meio do caminho entre o que o Professor Scarance (2009) chamou de um *hipergarantismo* e uma *repressão a todo custo*, sendo certo, no entanto, que esse equilíbrio não é algo tangível, constituindo-se, em verdade, numa meta, numa diretriz que deve nortear o processo penal[70]. Diante da dificuldade de traduzir o referido equilíbrio em textos de lei ou na aplicação concreta do direito, tem-se por meta não se distanciar do ponto médio entre a proteção à liberdade e a segurança da sociedade[71].

Não se trataria, portanto, de se construir um procedimento ideal que assegurasse de modo perene o equilíbrio desejável entre a segurança e a liberdade, o que seria incompatível com a variação de épocas e regiões, de tradições e culturas jurídicas, de ideologias e de sistemas políticos, mas de fixar algumas regras e princípios, os quais, em seu conjunto, constituiriam diretrizes fundamentais para a formação dos procedimentos[72].

E, no que se refere ao respeito às garantias do indivíduo, é preciso, para se atingir a meta de equilíbrio, que seja respeitado um *núcleo essencial de garantias*, por meio do qual devem ser asseguradas a imparcialidade, a ampla defesa e o contraditório[73].

Para Scarance Fernandes (2009), as expressões *eficiência*, *eficácia* e *efetividade* se ligam à ideia de produção de um efeito esperado ou consecução de um resultado pretendido. Nesse sentido, mede-se a *eficiência* pela aptidão do meio utilizado para atingir o resultado ou gerar o efeito; avalia-se a *eficácia* pelo alcance do resultado ou produção do efeito; e, por fim, constata-se a efetividade pela repercussão positiva do efeito ou do resultado em determinado âmbito social, político, econômico[74].

A verificação abstrata ou concreta da eficiência, eficácia ou efetividade de algo depende, essencialmente, da fixação de sua finalidade. No que se refere ao processo, sua finalidade seria permitir a todos os seus sujeitos o exercício de suas faculdades, de seus direitos, de suas garantias e de seus poderes[75]. A mesma análise que se deve fazer em relação ao processo penal pode ser feita em relação aos atos que compõem o procedimento e à atuação dos sujeitos da relação jurídica processual: eficiência, eficácia e efetividade da

[69] Ibid., p. 278.
[70] FERNANDES, 2009, p. 10.
[71] Ibid., p. 10.
[72] Id., 2008b, p. 11 e 15.
[73] Id., 2009, p. 11.
[74] Ibid., p. 10.
[75] FERNANDES, 2009, p. 10/11.

denúncia, da citação, de um meio de investigação e de produção de prova, da atuação do juiz, do promotor, do advogado[76].

A terceira concepção seria a necessidade de se promover uma análise à luz do princípio da proporcionalidade, como diretriz essencial para verificar eventuais excessos ou abusos na previsão e na utilização de meios especiais de investigação, já que estes poderão representar limitações a direitos ou garantias constitucionais[77].

O princípio da proporcionalidade em sentido amplo, também conhecido como princípio da proibição do excesso (*Übermassverbot*)[78] e princípio da razoabilidade[79], é amplamente admitido como critério doutrinário de avaliação da constitucionalidade de uma lei, ato ou decisão judicial.

Tem sua origem ligada à *law of land*, inscrita na Carta Magna de 1215 e, modernamente, sua positivação remonta à quinta e décima quarta emendas à Constituição

[76] FERNANDES, 2008b, p. 25 e _____, 2009, p. 11.
[77] FERNANDES, 2009, p. 11/12.
[78] CANOTILHO, p. 266/267.
[79] BARROSO, Luís Roberto. **Curso de direito constitucional contemporâneo**: os conceitos fundamentais e a construção do novo modelo. São Paulo: Saraiva, 2009, p. 255/256.

norte-americana[80]. Já no berço alemão, o princípio da proporcionalidade se desenvolveu no direito administrativo, funcionando como um limite à discricionariedade administrativa[81].

Para se aferir se determinada lei segue o princípio da proporcionalidade (*Verhältnismässigkeitsprincip*), deve-se verificar se atende aos seus três subprincípios (CANOTILHO, 2000) ou três máximas parciais (ALEXY, 2011), quais sejam, adequação ou conformidade (*Geeignetheit*), necessidade ou exigibilidade ou menor ingerência possível (*Erforderlichkeit*) e proporcionalidade em sentido estrito (*Verhältnismässigkeit*)[82].

Para ser adequada, uma medida adotada para realizar o interesse público deve ser apropriada à obtenção do fim pretendido, devendo haver prova dessa aptidão[83].

Para satisfazer a exigência da necessidade ou exigibilidade, a medida adotada deve ser o menos gravosa e onerosa possível para o cidadão. A doutrina acrescenta outros elementos voltados para uma maior operacionalidade prática deste subprincípio, quais sejam, (a) o da exigibilidade material, segundo o qual o meio deve ser o mais *comedido*[84] possível quanto à limitação dos direitos fundamentais, (b) o da exigibilidade espacial, que impõe a necessidade de se limitar o âmbito da intervenção, (c) o da exigibilidade temporal, que pressupõe a

---

[80] Amendment V - No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation; Amendment XIV - Section 1. All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws. Section 2. Representatives shall be apportioned among the several States according to their respective numbers, counting the whole number of persons in each State, excluding Indians not taxed. But when the right to vote at any election for the choice of electors for President and Vice-President of the United States, Representatives in Congress, the Executive and Judicial officers of a State, or the members of the Legislature thereof, is denied to any of the male inhabitants of such State, being twenty-one years of age,* and citizens of the United States, or in any way abridged, except for participation in rebellion, or other crime, the basis of representation therein shall be reduced in the proportion which the number of such male citizens shall bear to the whole number of male citizens twenty-one years of age in such State. Section 3. No person shall be a Senator or Representative in Congress, or elector of President and Vice-President, or hold any office, civil or military, under the United States, or under any State, who, having previously taken an oath, as a member of Congress, or as an officer of the United States, or as a member of any State legislature, or as an executive or judicial officer of any State, to support the Constitution of the United States, shall have engaged in insurrection or rebellion against the same, or given aid or comfort to the enemies thereof. But Congress may by a vote of two-thirds of each House, remove such disability. Section 4. The validity of the public debt of the United States, authorized by law, including debts incurred for payment of pensions and bounties for services in suppressing insurrection or rebellion, shall not be questioned. But neither the United States nor any State shall assume or pay any debt or obligation incurred in aid of insurrection or rebellion against the United States, or any claim for the loss or emancipation of any slave; but all such debts, obligations and claims shall be held illegal and void. Section 5. The Congress shall have the power to enforce, by appropriate legislation, the provisions of this article.

[81] BARROSO, 2009, p. 256.

[82] ALEXY, 2011, p. 116/117 e CANOTILHO, 2000, p. 269/270.

[83] CANOTILHO, 2000, p. 269/270.

[84] Ibid., p. 270: Canotilho utiliza, em vez de "comedido", o adjetivo "poupado".

rigorosa delimitação no tempo da medida coativa do poder público, e, por último, (d) o da exigibilidade pessoal, segundo o qual os interesses sacrificados deverão ser somente os da pessoa ou pessoas-alvo da medida[85].

Para atender ao princípio da proporcionalidade em sentido estrito[86], deve haver um equilíbrio entre o significado da intervenção para o atingido e os objetivos perseguidos pelo legislador[87]. Nas palavras de Canotilho (2000), deve-se pesar as desvantagens dos meios em relação às vantagens do fim, para daí se concluir se a medida é ou não proporcional em sentido estrito[88].

No Brasil, o princípio da proporcionalidade advém de construção doutrinária, o que difere de outros ordenamentos, como o português, em que a Constituição o prevê expressamente[89]. No direito constitucional alemão, é considerado norma constitucional não escrita[90].

Alexy (2011), que chama o princípio de a máxima da proporcionalidade, esclarece que não se trata, na realidade, de um princípio no sentido de mandamento de otimização, devendo suas três máximas parciais, a saber, adequação, necessidade e proporcionalidade em sentido estrito, ser tratadas como verdadeiras regras[91].

Segundo Gilmar Mendes, Inocêncio Coelho e Paulo Gustavo Branco (2008), a doutrina identifica como típica manifestação do excesso de poder legislativo a violação ao princípio da proporcionalidade ou da proibição do excesso, que se revela mediante a contraditoriedade, incongruência, irrazoabilidade ou inadequação entre meios e fins[92].

Portanto, a doutrina constitucional moderna, ao aferir os níveis de restrição que uma lei cria sobre um direito fundamental, preocupa-se em voltar olhos para o princípio da proporcionalidade, chegando a conceber, como uma forma evoluída do conhecido princípio

---

[85] Ibid., p. 270.
[86] Alexy se refere ao princípio da proporcionalidade em sentido estrito como o mandamento do sopesamento propriamente dito (ALEXY, 2011, p. 116/117).
[87] MENDES; COELHO; BRANCO, 2008, p. 332.
[88] CANOTILHO, 2000, loc. cit.
[89] Constituição da República Portuguesa: Art. 18º (Força jurídica) ... 2. A lei só pode restringir os direitos, liberdades e garantias nos casos expressamente previstos na Constituição, devendo as restrições limitar-se ao necessário para salvaguardar outros direitos ou interesses constitucionalmente protegidos. ... Art. 19º (Suspensão do exercício de direitos) ... 4. A opção pelo estado de sítio ou pelo estado de emergência, bem como as respectivas declaração e execução, devem respeitar o princípio da proporcionalidade e limitar-se, nomeadamente quanto às suas extensão e duração e aos meios utilizados, ao estritamente necessário ao pronto restabelecimento da normalidade constitucional.
[90] MENDES; COELHO; BRANCO, 2008, p. 330.
[91] ALEXY, 2011, p. 117.
[92] MENDES; COELHO; BRANCO, 2008, loc. cit.

da reserva legal, a exigência de um *princípio da reserva legal proporcional* (*Vorbehalt des verhältnismässigen Gesetzes*)[93].

Prosseguindo-se na análise do binômio *eficiência e garantismo*, destaca-se a necessidade, ao menos didática, de que se separe a criminalidade em três grupos, a saber, a criminalidade de bagatela e das infrações de menor potencial ofensivo, a criminalidade comum e a criminalidade grave ou organizada[94].

Essa classificação ganha importância para o presente estudo porque o último grupo, o da criminalidade grave ou organizada, constitui o ponto mais sensível da análise dos limites probatórios e investigatórios da atuação persecutória do Estado, já que, se, de um lado, o crime violento ou organizado cresce assustadoramente, alastrando o medo e a insegurança entre os cidadãos, de outro, não é incomum que se tragam propostas perigosas que representam risco de graves supressões das garantias individuais, de modo que atingir o equilíbrio entre a repressão ao crime organizado[95] e as garantias fundamentais do devido processo legal constituiria "o grande desafio contemporâneo"[96].

O presente trabalho é manifestação de aceitação desse desafio, que, de fato, é essencialmente contemporâneo, de modo que se analisará a interceptação das comunicações telemáticas, medida absolutamente fundamental para a eficiência da persecução da criminalidade organizada, buscando-se identificar, à luz dos diversos critérios até aqui expostos, os limites que se lhe devem ser impostos.

1.5 A busca da verdade e o processo penal constitucional

A linha de entendimento de que os direitos fundamentais seriam absolutos decorre de uma premissa jusnaturalista de que o Estado existiria para proteger os direitos naturais, como a vida, a liberdade e a propriedade[97]. No entanto, se assim fosse, nenhuma medida de interesse público que dependesse de acesso a dados íntimos ou privados do indivíduo poderia ser

[93] Ibid., p. 331/332.
[94] FERNANDES, 2008a, p. 226.
[95] Benjamim Silva Rodrigues lança a pergunta "quem não fica fascinado, perante a ameaça do crime organizado, pela possível eficácia de 'pequenas' ou inclusive 'grandes' restrições no segredo das comunicações, mas ao mesmo tempo também alarmado numa óptica do Estado de Direito?" (RODRIGUES, 2009, p. 18).
[96] FERNANDES, 2008a, p. 227/228.
[97] MENDES; COELHO; BRANCO, 2008, p. 240.

implementada pelo Estado, podendo-se, diante disso, adotar a premissa de que a inviolabilidade da intimidade e da vida privada não é absoluta.

É notório que tal direito, em determinadas situações, entrará em colisão com outros princípios constitucionais. Para introduzir esta concepção, é fundamental a compreensão do conceito de direito à proteção e sua distinção do conceito de direito de defesa.

Os direitos a proteção são direitos a ações positivas do Estado, impondo-se a este o zelo para que terceiros não intervenham na esfera do indivíduo, enquanto os direitos de defesa impõem ao Estado ações negativas, ou seja, protegem o indivíduo contra intervenções do próprio Estado[98]. Os bens jurídicos a serem protegidos pelas normas contendo direitos à proteção seriam, segundo Alexy (2011), todos os que sejam dignos de proteção do ponto de vista dos direitos fundamentais, como a dignidade, a liberdade, a família e a propriedade, o que deverá ser implementado pelo Estado através das mais diversificadas formas, a exemplo de normas de direito penal, de responsabilidade civil, de direito processual e por meio de atos administrativos e ações fáticas[99].

A Constituição brasileira contém diversos dispositivos prevendo direitos à proteção, podendo-se citar, além dos chamados mandamentos constitucionais de criminalização[100], o direito à segurança, inscrito no *caput* do artigo 5º, que se apresenta como um princípio[101], que pode entrar em colisão com o princípio da inviolabilidade da intimidade e da vida privada (art. 5º, X).

Sobre esta possível colisão, deve-se observar que os princípios são normas que exigem a realização de algo, da melhor forma possível, de acordo com as possibilidades fáticas e jurídicas. Daí se dizer que princípios são mandamentos de otimização, que podem coexistir, permitindo o balanceamento de valores e interesses, consoante seu peso e a ponderação de outros princípios[102]. Por isso, em caso de conflito entre princípios, é possível que mais de um se aplique, com acentuações diversas[103].

Esta colisão, segundo Alexy (2011), se resolve estabelecendo-se uma *relação de precedência condicionada* entre os princípios, com base nas circunstâncias do caso concreto,

---

[98] ALEXY, 2011, p. 456.
[99] Ibid., p. 450.
[100] Mendes, Coelho e Branco mencionam, no artigo 5º, os incisos XLI, XLII, XLIII, XLIV, no artigo 7º, o inciso X, além do artigo 227, §4º e do artigo 225, §3º (MENDES; COELHO; BRANCO, 2008, p. 582/583).
[101] Ver item 2.1.1, *supra*, sobre a distinção entre regras e princípios.
[102] CANOTILHO, 2000, p. 1161: As regras, diferentemente – diz o autor –, impõem, permitem ou proíbem imperativamente uma conduta, obedecendo à lógica do tudo ou nada e excluindo-se quando diante de uma antinomia.
[103] Ibid., p. 1182.

de modo a se fixar condições para que um princípio prevaleça sobre outro, o que se aplicará somente àquela situação, pois, sob outras condições, a solução poderia ser outra[104].

Em palestra proferida no Brasil, Alexy (1998) classificou de colisão em sentido estrito aquela ocorrente somente entre direitos fundamentais e a de colisão em sentido amplo aquela que se dá entre direitos fundamentais e outros princípios ou valores voltados para a proteção dos interesses da comunidade[105], aplicando-se este último conceito, segundo aqui concluímos, à colisão entre a inviolabilidade à intimidade e à vida privada e o princípio da segurança e os mandamentos de criminalização.

E, segundo Canotilho (2000), essa colisão de direitos fundamentais ocorreria, não só entre direitos individuais de diferentes titulares (colisão autêntica), mas também entre direitos individuais do titular e bens jurídicos da comunidade (colisão não autêntica)[106].

Portanto, tem-se que, quando o interesse na persecução penal, tutelado pelo princípio da segurança[107], a ser proporcionada pelo Estado, e os objetivos dos mandamentos de criminalização entram em colisão com o princípio da inviolabilidade da intimidade e da vida privada, se está diante de uma colisão *em sentido amplo* (ALEXY, 2011) e *não autêntica* (CANOTILHO, 2000) a ser resolvida condicionadamente conforme a situação concreta se apresentar.

Um dos mecanismos voltados para dar concretude ao princípio da segurança e aos mandamentos de criminalização[108] é a persecução penal, que, não se resumindo à fase judicial do processo penal, é precedida de uma fase investigatória[109].

Será nessa fase investigatória que, via de regra, terá lugar o uso da interceptação das comunicações telemáticas, embora haja previsão de sua utilização também na fase judicial.

A interceptação das comunicações telemáticas, enquanto mecanismo comumente utilizado na fase pré-processual, tem por objetivo a reunião de elementos probatórios que permitam a reconstrução histórica de um fato criminoso ou, como outros preferem, a busca da verdade[110], tanto para a viabilização da inauguração da fase de persecução penal em juízo,

---

[104] ALEXY, 2011, p. 96.
[105] Palestra proferida por Robert Alexy na Fundação Casa de Rui Barbosa, intitulada "Kollision und Abwägung als Grundproblem der Grundrechtsdogmatik", Rio de Janeiro, 10.12.1998 apud MENDES; COELHO; BRANCO, 2008, p. 342.
[106] CANOTILHO, 2000, p. 1270/1271.
[107] No Brasil, o princípio da segurança está inscrito no *caput* do artigo 5º da CF.
[108] No Brasil, há mandamentos de criminalização no art. 5º, XLI, XLII, XLIII e XLIV, art. 7º, X e art. 227, §4º e art. 225, §3º, todos da CF.
[109] Ressalva-se, contudo, que é pacífica a dispensabilidade da investigação para que se possa inaugurar a fase judicial da persecução, desde que os autos contenham elementos mínimos a demonstrar a materialidade e a autoria do delito.
[110] Bastante controvertido é o conceito de verdade no processo penal. O mito da busca de uma "verdade real", engendrado nos meandros da inquisição, e que, por não se conhecer a idéia de limites, levou muitos a confessar

quanto para indicar caminhos e elementos que poderão ter valor probatório no momento do julgamento.

Nesse ponto, é de fácil percepção a relação da interceptação das comunicações telemáticas com a necessidade de se impor ao Estado o dever de 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.

Pode-se dizer que tais limites serão os direitos e garantias[111] individuais que incidem no processo penal e que sejam aplicáveis também à fase investigatória[112]. É nesse sentido que Tucci fala em *devido processo penal*, como uma vertente do devido processo legal constitucionalmente previsto, que reclama, para a sua efetivação, a observância rigorosa das formalidades prescritas em lei para o perfeito atingimento de sua finalidade solucionadora do conflito entre o interesse punitivo e a liberdade[113].

Para além disso, a visão de processo penal constitucional eleva o indivíduo que venha a ser alvo do interesse punitivo estatal de uma condição de objeto de investigação à de sujeito de direitos ou sujeito do processo, armado com o seu direito de defesa e com as suas garantias individuais[114].

Deve-se ter claro, portanto, que a busca da verdade deverá respeitar a esfera de proteção do indivíduo sob pena de dar causa, dependendo de qual tenha sido a conduta excessiva ou arbitrária, à punição dos agentes que se excederam e, principalmente, à ilicitude do material probatório coletado[115].

---

não só delitos não cometidos, mas também alguns impossíveis de serem realizados, está intimamente relacionado com a estrutura do sistema inquisitório, com o "interesse público" (cláusula geral que serviu de argumento para as maiores atrocidades), chegando, em alguns períodos, a legitimar a tortura (LOPES JR., Aury. **Direito processual penal e sua conformidade constitucional**. v. I. 3ª ed. Rio de Janeiro: Lumen Juris, 2008, p. 521/524). Fala-se hoje em verdade processual. Para Ferrajoli o conceito de verdade processual é, na realidade, uma verdade aproximativa, que não pretende ser, efetivamente, a verdade, devendo ser obtida com o respeito aos procedimentos e garantias da defesa (FERRAJOLI, Luigi. **Derecho y razón**: teoria del garantismo penal. 2ª ed. Tradução Perfecto Andrés Ibáñez et al. Madri: Trotta, 1997, p. 50), visando "a maior aproximação possível" (UBERTIS, Giulio. **La prova penale**: profili giuridici ed epistemologici. Torino: Utet, 1999, p. 10) de uma certeza.

[111] Ver a diferenciação entre direitos e garantias no item 1.2, *supra*.

[112] Sobre a existência de um direito à investigação decorrente do direito à prova, ver o próximo item (1.6).

[113] TUCCI, Rogério Lauria. **Direitos e garantia individuais no processo penal brasileiro**. 3ª ed. rev. atual. e ampl. São Paulo: Revista dos Tribunais, 2009, p. 75.

[114] FERNANDES, Antonio Scarance. **Processo penal constitucional**. 6ª ed. rev. atual. e ampl. São Paulo: Revista dos Tribunais, 2010, p. 22.

[115] Ibid., p. 89.

1.6 O direito à investigação como vertente do direito à prova

Sabe-se que é direito subjetivo das partes introduzir o material probatório no processo, bem como participar nas fases do respectivo procedimento, não bastando que lhes seja assegurada a mera apresentação de pretensões sem meios efetivos de influir sobre o convencimento do juiz[116]. Dessa forma, ao direito da parte de apresentar provas corresponde um dever do magistrado, já que, evidentemente, de nada serviria assegurar às partes o direito à prova, se o juiz pudesse deixar de apreciá-las e valorá-las, no momento do julgamento[117].

E esse ciclo se aperfeiçoa com o dever de motivação das decisões judiciais, assegurado pelo artigo 93, IX da CF. Nas palavras de Antonio Scarance Fernandes (2010), os destinatários da motivação não são mais somente as partes e os juízes de segundo grau, mas também a comunidade que, com a motivação, tem condições de verificar se o juiz, e por consequência a própria Justiça, decide com imparcialidade e com conhecimento de causa.

É por meio da motivação que se avalia o exercício da atividade jurisdicional[118]. O dever de motivação se apresenta, portanto, em última análise, como meio de assegurar o efetivo respeito a diversos direitos, inclusive o direito à prova.

E esse direito, à prova, naturalmente, não deve ser assegurado apenas ao acusado, mas também ao titular do direito de ação, ao qual caberá a iniciativa da persecução[119], bem como não deve se restringir a aspectos endoprocessuais, já que há elementos probatórios que se formam fora ou antes do processo, como aqueles que se prestam a demonstrar o *fumus comissi delicti* para o próprio início da persecução. Portanto, uma das vertentes do direito à prova é o direito à investigação, pois a faculdade de procurar e descobrir provas se apresenta como condição indispensável para seu exercício[120-121].

É por força dessa vertente do direito à prova que se viabiliza, sob certas condições, a restrição de direitos fundamentais do indivíduo, como resultado do princípio da convivência das liberdades públicas, que não podem ser entendidas em sentido absoluto, pelo que não se

---

[116] GOMES FILHO, Antonio Magalhães. **Direito à prova no processo penal**. São Paulo: Revista dos Tribunais, 1997, p. 84.
[117] GRINOVER, Ada Pellegrini. O conteúdo da garantia do contraditório. In: **Novas tendências do direito processual**. Rio de Janeiro: Forense Universitária, 1990, p. 31.
[118] FERNANDES, 2010, p. 127.
[119] GOMES FILHO, 1997, loc. cit.
[120] Ibid., p. 86.
[121] Sobre o direito de investigação pela defesa ver MACHADO, André Augusto Mendes. **Investigação criminal defensiva**. 2009. 207 f. Dissertação (Mestrado em Processo Penal) – Faculdade de Direito, Universidade de São Paulo, São Paulo, 2009.

permite que qualquer delas seja exercida de modo danoso à ordem pública e às liberdades alheias[122] .

A intimidade e a privacidade, como direitos fundamentais que são, se apresentam como limites, de índole extraprocessual ou política, à atividade probatória[123].

Damaska (1973) identificou dois critérios de limites probatórios: o primeiro dependente da análise da relevância da prova, pois provas como *hearsay* e a utilização dos antecedentes criminais do réu poderiam dificultar a busca da verdade, na medida em que seu impacto sobre o julgador poderia acabar sendo mais forte do que seu efetivo valor probatório; e o segundo voltado a verificar a obediência a formalidades na obtenção da prova[124].

Para o presente estudo, interessa a análise deste último critério, já que será por meio dele que se poderá analisar os níveis de restrição aos direitos fundamentais à intimidade e à privacidade promovidos pela medida de interceptação telemática.

1.7 Interceptação telemática: natureza jurídica

A definição da natureza jurídica da interceptação telemática dependerá da compreensão prévia da distinção entre meio de prova e fonte de prova, bem como entre meio de prova e meio de obtenção de prova, também chamada meio de busca de prova.

Antes de se passar a este ponto, deve-se verificar a diferença entre prova direta e prova indireta[125]. Segundo Carnelutti (2001), a primeira é aquela cujo objeto de prova ou o fato a provar coincide com o objeto de percepção pelo juiz e a última aquela em que não há essa coincidência, ou seja, aquela em que o fato submetido à percepção do juiz serve apenas como um meio para ele conhecer o fato que se deseja provar[126].

---

[122] GRINOVER, Ada Pellegrini. Interceptações telefônicas e gravações clandestinas no processo penal. In: **Novas tendências do direito processual de acordo com a Constituição de 1988**. 2ª ed. Rio de Janeiro: Forense Universitária, 1990, p. 60.

[123] GOMES FILHO, 1997, p. 93: Diz o autor que os limites processuais (lógicos, epistemológicos) são os que excluem provas impertinentes, irrelevantes ou que possam conduzir o julgador a uma avaliação errônea.

[124] DAMASKA, Mirjan Radovan. **Evidentiary Barriers to Conviction and Two Models of Criminal Procedure**: A Comparative Study. Faculty Scholarship Series. Paper 1591, 1973, p. 514.

[125] Não se está referindo à distinção entre a prova (que se refere diretamente ao fato a ser provado) e o indício (que se liga ao fato a ser provado por raciocínio indutivo), este último também chamado de prova semi-plena ou incompleta (GRINOVER, Ada Pellegrini; GOMES FILHO, Antonio Magalhães; FERNANDES, Antonio Scarance. **As nulidades no processo penal**. 11ª ed. São Paulo: Revista dos Tribunais, 2009, p. 113).

[126] CARNELUTTI, Francesco. **A prova civil**. Tradução Lisa Pary Scarpa. Campinas: Bookseller, 2001, p. 83.

Nesse sentido, tem-se que raras serão as provas diretas, podendo-se citar a inspeção judicial, por meio da qual o julgador constata pessoalmente determinado fato. Nas provas indiretas, a exemplo do testemunho oral, dá-se a necessidade de uma operação complexa de percepção e dedução (pelo juiz)[127].

Exposta tal diferença, fica mais simples a compreensão da distinção entre fontes de prova e meios de prova. As primeiras, fontes de prova, são todas as formas, anteriores à existência do processo, de esclarecer a ocorrência de um fato, aí incluídas as pessoas que o presenciaram, os registros do evento em meio audiovisual e os vestígios, enquanto os meios de prova são os métodos pelos quais essas fontes são incorporadas ao processo, a exemplo, nas palavras de Paolo Tonini (2002), da prova testemunhal, da oitiva das partes, das acareações, dos reconhecimentos, das reconstituições judiciais, da perícia e da prova documental[128].

Para o presente estudo, importa, também, distinguir os meios de prova dos meios de obtenção de prova ou meios de pesquisa de prova. Enquanto os primeiros constituem os instrumentos que, a exemplo dos documentos, depoimentos de testemunhas e exames periciais, levam os fatos ao conhecimento dos sujeitos processuais, os últimos são as próprias medidas voltadas a coletar, obter, buscar os elementos que serão, posteriormente, transportadas até o processo, a exemplo da busca e apreensão, interceptação telefônica e quebras de sigilo bancário e fiscal[129].

Há, ainda, a distinção entre atos de prova e atos de investigação, sendo os primeiros aqueles praticados perante o juiz, dirigidos a convencê-lo de algo, para o julgamento final, estando a serviço do processo e da sentença e exigindo estrita observância da publicidade, contradição e imediação, enquanto os atos de investigação seriam os realizados na investigação preliminar, que se refeririam não a uma afirmação, mas a uma hipótese[130].

Diante disso, pode-se afirmar que a medida de interceptação é uma providência cautelar[131] que constitui um meio de obtenção de prova[132-133], tendo como resultados uma

---

[127] BADARÓ, Gustavo Henrique Righi Ivahy. **Ônus da prova no processo penal**. São Paulo: Revista dos Tribunais, 2003, p. 163/164.

[128] artigos 194 a 243 do CPP italiano (TONINI, Paolo. **A prova no processo penal italiano**. Tradução Alexandra Martins e Daniela Mróz. São Paulo: Revista dos Tribunais, 2002, p. 108/109).

[129] BADARÓ, Gustavo Henrique Righy Ivahy. **Processo penal**. Rio de Janeiro: Elsevier, 2012, p. 270/273; TONINI, 2002, p. 242/243; ZILLI, Marcos Alexandre Coelho. **A iniciativa instrutória do juiz no processo penal**. São Paulo: Revista dos Tribunais, 2003, p. 183.

[130] LOPES JR., 2008, p. 500.

[131] FERNANDES, 2010, p. 96.

[132] Grinover, Gomes Filho e Scarance Fernandes, no entanto, afirmam que a doutrina enquadra as interceptações telefônicas na coação processual *in re* e as considera meio de apreensão imprópria, no sentido de por elas se apreenderem os elementos fonéticos que formam a conversa telefônica." (GRINOVER; GOMES FILHO; FERNANDES, 2009, p. 165). Luiz Flavio Gomes e Raúl Cervini se filiam à posição de Grinover, Gomes Filho e

fonte de prova[134] e o material coletado, que estará contido numa mídia, como CD ou DVD, um meio de prova documental[135], que será inserido no processo.

Ressalva-se, contudo, a rara hipótese de interceptação decretada no curso do processo, para fins de instrução processual penal, o que, no Brasil, aliás, encontra respaldo constitucional (art. 5º, XII, CF) e infraconstitucional (art. 1º, Lei 9.296/96). Nesse caso, estar-se-ia, da mesma forma, diante de meio de obtenção de prova, mas não de ato de investigação. Tratar-se-ia de ato de prova, voltado para influir diretamente na sentença, apesar de as garantias da publicidade e contraditório tornarem-se diferidas.

Mas há que se fazer uma ponderação quanto à possibilidade de interceptação na fase processual. Apesar de o juiz poder, no curso do processo, decretar medidas cautelares até de ofício, aí incluída a prisão preventiva do réu, que vem a ser a mais extrema das medidas, é de se destinar às interceptações das comunicações tratamento diverso daquele destinado às cautelares. As medidas cautelares, no processo penal, podem ser pessoais ou patrimoniais[136], sendo exemplos das primeiras a prisão preventiva (arts. 312 a 315 do Código de Processo Penal - CPP) e as medidas alternativas à prisão (arts. 319 e 320 do CPP) e exemplos das últimas o sequestro de bens imóveis (arts. 125 a 131 do CPP), o sequestro de bens móveis (art. 132 do CPP), a especialização e registro da hipoteca legal (art. 134 e 135 do CPP), o arresto de bens imóveis prévio ao registro e especialização da hipoteca legal (art. 136 do CPP) e o arresto subsidiário de bens móveis (art. 137 do CPP)[137].

Já a interceptação das comunicações telemáticas se constitui, como concluído acima, num meio de obtenção de prova, que, por sua própria natureza, é incompatível com o exercício do contraditório pleno, já que somente tem condições de atingir sua finalidade se

---

Fernandes, mas, de modo semelhante ao que aqui se conclui, afirmam que "a finalidade da interceptação telefônica, em suma, como já se afirmou, é, antes de tudo, a obtenção de uma 'prova', que se materializa num documento (auto circunstanciado, transcrição) ou num depoimento (prova testemunhal)" (GOMES, Luiz Flavio. Interceptação telefônica e "encontro fortuito" de outros fatos. In: **Boletim do Instituto Brasileiro de Ciências Criminais**, São Paulo, n. 51, p. 6, fev. 1997, p. 116).

[133] Segundo a classificação adotada por Aury Lopes Jr., a medida de interceptação telemática é um ato de investigação (LOPES JR., 2008, p. 500).

[134] GRINOVER, GOMES FILHO; FERNANDES, 2009, p. 165: "O resultado da interceptação – que é uma operação técnica – é fonte de prova."

[135] GRINOVER; GOMES FILHO; FERNANDES, 2008, p. 165: "Meio de prova será o documento (a gravação e sua transcrição) a ser introduzido no processo." Para Lopes Jr., o conceito de documento incluiria qualquer escrito, fitas de áudio, vídeo, fotografias, tecidos e objetos móveis que fisicamente possam ser incorporados ao processo e que desempenham uma função persuasiva (probatória) (LOPES JR., 2008, p. 636/637); no artigo 234 do Código de Processo Penal italiano, "É consentita l'acquisizione di scritti o di altri documenti che rappresentano fatti, persone o cose mediante la fotografia, la cinematografia, la fonografia o qualsiasi altro mezzo."; e, para Tonini: "Ebbene, i documenti si qualificano appunto come prove precostituite e, pertanto, si pongono come eccezioni alia regola dell'immediatezza." (TONINI, Paolo. **La prova penale**. 4ª ed. Padova: Cedam, 2000, p. 190).

[136] BADARÓ, 2012, p. 710.

[137] BADARÓ, 2012, p. 701/702.

sua implementação não for de conhecimento da pessoa que tem as suas comunicações monitoradas. Ocorre que a implementação de medida com essas peculiaridades no curso do processo violaria o princípio da paridade, porquanto, em tal fase, o investigado já ostentará a condição de sujeito processual, acusação e defesa se encontrarão em pleno exercício da dialética baseada em contraditório pleno e o acusado, não raro, travará constantes diálogos sobre suas estratégias defensivas, e não necessariamente só com seu defensor (pois neste caso a imprestabilidade probatória do diálogo captado seria óbvia, por força do art. 7º, II da Lei 8.906/94).

Afinal, a autodefesa, com duplo aspecto, se compõe do direito de audiência e do direito de presença, sendo o primeiro a possibilidade que o acusado tem de influir sobre a formação do convencimento do juiz por meio de seu interrogatório e o segundo a sua oportunidade de tomar posição, a todo momento, acerca das alegações e provas produzidas, gozando o acusado da garantia da imediação com o juiz e com as provas[138]. E, para viabilizar a real participação das partes na relação jurídica processual, o contraditório há que ser pleno e efetivo, o que evidencia a relação entre o contraditório e o princípio da igualdade, que será instrumento de eliminação de qualquer desigualdade, jurídica ou de fato, entre os sujeitos do processo[139].

Além disso, para os que sustentam a impossibilidade de interceptação deferida a pedido da defesa[140], a implementação da medida no curso da instrução processual geraria desequilíbrio das forças, faculdades e prerrogativas processuais em prejuízo do réu, na medida em que este não poderia adotar igual medida.

Para Maria Lucia Karam (2012), não se autoriza, no curso do processo, prova produzida sem o conhecimento do réu, sob pena de rompimento com as garantias do contraditório e da ampla defesa, concretizadoras da fórmula fundamental do devido processo legal[141].

Também Roberto Delmanto e Roberto Delmanto Jr. (1996) entendem que a interceptação telefônica durante a instrução judicial colide com as garantias constitucionais da igualdade, do contraditório, da ampla defesa, bem como com o direito à lealdade processual, abrangido pela garantia do devido processo legal e com a própria inviolabilidade do exercício da advocacia (art. 133), esta última no caso de interceptação de comunicação telefônica entre

---

[138] GRINOVER, 1990a, p. 10.
[139] GRINOVER, 1990a, p. 11.
[140] Abordaremos a possibilidade de interceptação deferida a pedido da defesa no item 4.6.
[141] KARAM, Maria Lucia. **Interceptação de comunicações telefônicas**: o Estado máximo, vigilante e onipresente. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/anexos/10286-10286-1-PB.html>. Acesso em: 10 Mar. 2012.

o acusado e seu defensor. Afirmam que o tratamento desigual às partes se mostra mais evidente com o fato de a lei ordinária não ter previsto a possibilidade da defesa também requerer a interceptação de comunicação telefônica de terceiros que tenham relação com o processo, como a vítima e testemunhas de acusação, caso existam indícios de que tenham faltado com a verdade ou omitido dados relevantes para a apuração da verdade material, objetivo maior do processo penal. Entendem que não se pode considerar leal uma prova feita a pedido ou com o conhecimento de uma parte, e com a participação desta, sem a ciência e participação da outra[142].

Além disso, como observado acima por Aury Lopes Jr. (2008), os atos de prova, aqueles praticados perante o juiz, exigem estrita observância da publicidade, elemento que não se faria presente em caso de interceptação realizada no curso da instrução processual[143].

Em Portugal, há previsão legal expressa vedando a medida na fase processual[144]. Mas, no Brasil, ainda que procedentes sejam os fundamentos para vedar a interceptação das comunicações na fase processual, como sustentar tal entendimento à luz do teor do dispositivo constitucional "*nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal*"?

Para Roberto Delmanto e Roberto Delmanto Jr. (1996), "*enquanto não revogada a permissão constitucional, ... para evitar a violação de garantias individuais, melhor seria que a lei ordinária tivesse limitado essa interceptação à fase do inquérito policial, onde, no entender da maioria da doutrina, não haveria o contraditório*"[145].

Assume-se aqui que, não tendo a lei ordinária promovido a limitação acima idealizada por Roberto Delmanto, a interpretação mais equilibrada da expressão constitucional "instrução processual penal", é a de que o produto da diligência de interceptação de comunicações poderá ser utilizado para fins probatórios na fase processual, porém a medida somente poderá ser implementada, executada na fase preliminar.

Do contrário, haveria violação ao núcleo essencial de garantias[146], na medida em que a imparcialidade do julgador sofreria danos e, *in casu*, danos com efeitos mais danosos ao indivíduo do que aqueles decorrentes da perda de imparcialidade que o magistrado possa

---

[142] DELMANTO, Roberto; DELMANTO JR., Roberto. A permissão constitucional e a nova lei de interceptação telefônica **Boletim do Instituto Brasileiro de Ciências Criminais**, São Paulo, n. 47, p. 2, out. 1996.
[143] LOPES JR., 2008, p. 500.
[144] Lei 109 de 15 de setembro de 2009. Art. 18(2). A intercepção e o registo de transmissões de dados informáticos só podem ser autorizados durante o inquérito, se houver razões para crer que a diligência é indispensável para a descoberta da verdade ou que a prova seria, de outra forma, impossível ou muito difícil de obter, por despacho fundamentado do juiz de instrução e mediante requerimento do Ministério Público.
[145] DELMANTO; DELMANTO JR., 1996, p. 2.
[146] Sobre o núcleo essencial de garantias, ver item 1.4, *supra*.

sofrer quando defere a medida na fase investigatória, porquanto em momento mais distante da sentença, ocorrendo, por consequência, um afastamento do ponto médio existente entre a proteção à liberdade e a segurança da sociedade.

2 COMUNICAÇÃO TELEMÁTICA, INTERNET E OS MEIOS MODERNOS DE INTERCEPTAÇÃO

2.1 Comunicação telemática e internet

Antes de tratar de comunicação telemática, importa compreender o conceito de telecomunicação, que, segundo o artigo 60, §1º da Lei 9.472/97[147], 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."

Para o espanhol Juan José González López (2007), telecomunicação é toda forma de comunicação a distância que se realize por meio de um artifício técnico eletromagnético ou luminoso, aí incluídas, portanto, as comunicações telefônicas, telegráficas e telemáticas, bem como as de rádio e televisão[148].

Há três elementos presentes nas telecomunicações: a infraestrutura, os meios de transmissão e o conteúdo transmitido[149].

A infraestrutura são os componentes físicos empregados para efetuar a comunicação, a saber, os cabos (de cobre, coaxial e de fibra ótica), os emissores de ondas hertzianas e os satélites. Cabos são infraestruturas terrestres, enquanto emissores de ondas hertzianas e satélites são aéreos. Dentre as terrestres, os cabos de cobre são usados, tradicionalmente, para a telefonia fixa, muito embora venham sendo abandonados, em razão de sua *limitação de banda*, ou seja, sua limitada capacidade de conduzir sinais avançados de telefonia e multimídia. O cabo coaxial é próprio para sinal de televisão e serviço de internet e o de fibra ótica vem substituindo o cabeamento de cobre, por ser menos suscetível de falhas e mais seguro. Os emissores de ondas hertzianas conduzem sinais de rádio e televisão, mas têm desempenhado importante papel também na telefonia móvel. O satélite desempenha o mesmo papel desses emissores, com a diferença de que gravita na órbita da Terra[150].

---

[147] 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.
[148] LÓPEZ, Juan José González. **Los datos de tráfico de las comunicaciones electrónicas en el proceso penal**. Madrid: La Ley, 2007, p. 30.
[149] LÓPEZ, 2007, p. 31.
[150] LÓPEZ, 2007, p. 31/32.

Os meios de transmissão são o modo como a informação viaja através das infraestruturas acima listadas. Nesse sentido, nos cabos de cobre e coaxiais, viajam ondas eletromagnéticas; nos de fibra ótica, viajam os impulsos luminosos; nas infraestruturas aéreas, as ondas hertzianas[151].

E, finalmente, o conteúdo da transmissão é a informação, que pode consistir em sinais, textos, imagens ou áudios, podendo ser transportada de forma digital ou analógica[152-153].

Portanto, o conteúdo da transmissão será o conteúdo pretendido pelos interlocutores. Digital ou analógica será apenas a forma pela qual esse conteúdo viajará.

Quanto ao conceito de comunicação telemática, há um consenso no entendimento de que a expressão "telemática" advém da conjunção dos termos "telecomunicações" e "informática"[154].

É verdade, como observam Gomes e Cervini (1997), que, hoje, praticamente todas as formas de telecomunicações já estão conjugadas com a informática, processo que se teria iniciado em 1974 com o sistema telefônico inteligente unido com microprocessadores[155], mas não basta, para se classificar como telemático um determinado meio de comunicação, que haja, no curso de todo o processo comunicativo, a atuação de algum sistema informatizado.

Não se pode, por exemplo, classificar de telemática a comunicação realizada através de cabos de telefonia fixa, inteiramente baseada em ondas eletromagnéticas, sem depender da conversão do conteúdo humano em sinais binários, pelo só fato de que o avanço tecnológico

---

[151] Ibid., p. 32.
[152] Ibid., p. 32.
[153] Segundo o *Oxford Dictionary*, digital é uma qualidade de sinais ou dados expressos em uma série de dígitos 0 ou 1, usualmente representados por valores de uma quantidade física tal como voltagem ou polarização magnética. O termo é usualmente empregado como oposto de analógico. O sinal da TV digital é um exemplo, como o nome sugere, de transmissão digital de dados. Diz o verbete original: "Digital. *Adjective*. 1[of signals or data] expressed as series of the digits 0 and 1, typically represented by values of a physical quantity such as voltage or magnetic polarization. Often contrasted with analogue. 2 relating to, using, or storing data or information in the form of digital signals: digital TVa digital recording." (OXFORD Dictionaries Online. Oxford University Press. Disponível em: <http://oxforddictionaries.com/definition/english/digital>. Acesso em: 10 set. 2013). Assim, quando algum processo comunicativo passa pela conversão do conteúdo humano em um código chamado binário, porquanto composto de 0 e 1, a comunicação pode ser classificada de digital. No princípio da comunicação instantânea a distância, não foi preciso usar tal tipo de tecnologia, podendo-se citar como exemplos o telégrafo, tanto o manual quanto o elétrico, e o telefone, que não necessitavam da conversão do conteúdo natural em sinal digital para que ocorresse a transmissão da informação: a voz era convertida, simplesmente, em sinais elétricos (HUURDEMAN, Anton. A., **The worldwide history of telecommunications**. Hoboken: John Wiley & Sons, Inc., 2003, p. 156), sendo, posteriormente, convertida novamente em áudio para ser ouvida pelo receptor, ou seja, procedimento inteiramente analógico.
[154] LÓPEZ, 2007, p. 33: "El concepto 'telemática' procede de la combinación de los vocablos 'telecomunicaciones' e 'informática' y designa 'todo lo que tiene que ver con la comunicación entre ordenadores, tanto en entornos locales como en entornos más amplios'"; GOMES, 1997, p. 165: "Sucintamente, telemática é telecomunicação (qualquer uma das variadas formas) mais informática."; e Novo Dicionário Eletrônico Aurélio, versão 7.0, 5ª. ed., 2010: "De *tele(comunicação)* + *(infor)mática*.] Substantivo feminino. 1. Ciência que trata da manipulação e utilização da informação através do uso combinado de computador e meios de telecomunicação."
[155] GOMES; CERVINI, p. 165

substituiu a antiga central telefônica manual, em que a conexão entre os interlocutores dependia de operadores humanos plugando um fio no outro, por centrais automatizadas. Aliás, a própria automação das centrais percorreu longos caminhos até se poder falar em informatização de seu funcionamento.

Depois da manual, surgiu a central eletromecânica, cujos mecanismos reagia a sinais elétricos enviados conforme os usuários discavam números.

Em 1950, toda a telefonia dos Estados Unidos já funcionava à base de centrais telefônicas eletromecânicas, exceto para chamadas de longa distância, que ainda dependiam de intervenção de operadores. Em 1965, aboliu-se completamente a necessidade de operadores humanos[156].

Da chamada *manual telefone switchboard* evoluiu-se para a *electromechanical telephone switching*, que substituiu a primeira[157].

A possibilidade de informatizar as centrais telefônicas foi percebida por engenheiros desenvolvedores dos primeiros computadores, tendo em vista a semelhança do processo de funcionamento daquelas com o dos computadores[158].

Em 1965, a empresa americana AT&T pôs em funcionamento a primeira central telefônica eletrônica, a *#1 Electronic Switching System* (ESS)[159].

As transmissões sem fio começaram a surgir antes disso, em 1866, quando se constatou que a Terra é cercada por uma camada de eletricidade estática, através da qual ondas poderiam ser propagadas, primeiro ondas elétricas e, mais tarde, eletromagnéticas[160].

Mas, mesmo depois de tudo isso, a essência do processo comunicativo ainda não envolvia conversão do conteúdo humano, objeto da transmissão, em sinais binários, não se podendo, portanto, classificá-lo de digital.

Foi no início da década de 1980, coincidindo com o desenvolvimento da fibra ótica, que se começou a implementar sistemas de transmissão digitais[161].

São estas as comunicações, as realizadas através da transmissão de sinais digitais, binários, que se podem classificar de telemáticas.

---

[156] IEEE Global History Network. Disponível em: <http://www.ieeeghn.org/wiki/index.php/Telephone_switching>. Acesso em: 01 ago. 2013.
[157] Ibid.
[158] Ibid.
[159] HOCHHEISER, Sheldon. **Stars**: Electromechanical telephone switching, p. 2299/2305, vol. 101, n. 10, October 2013 Proceedings of the IEEE, p. 2305. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=06600843>. Acesso em: 15 set. 2013.
[160] HURRDEMAN, 2003, p. 200.
[161] ENCYCLOPÆDIA BRITANNICA. Disponível em: <http://www.britannica.com/EBchecked/topic/585993/telephone/279924/Transmission?anchor=ref1117804>. Acesso em: 12 set. 2013.

Mas há uma questão que obriga a restrição da conclusão acima ao segmento das telecomunicações, excluindo-a das análises jurídicas ou processuais penais. É que, hoje em dia, há uma tendência à digitalização de todos os tipos de comunicação, ainda que seja somente na fase de emissão e de recepção[162], de modo que se pode afirmar que grande parte das comunicações atuais via rádio, telefonia fixa e telefonia móvel se dão de forma digital.

Se não se impuser tal reserva à assertiva, concluir-se-ia que muitas das comunicações telefônicas realizadas hoje são, na realidade, telemáticas, porquanto operando com base em transmissão de sinais binários.

Veja-se que, na legislação federal norte-americana, a definição de *electronic communication* (a transferência de sinais, texto, imagens, sons, dados ou inteligência de qualquer natureza transmitida, total ou parcialmente, por cabo, rádio ou sistema eletromagnético, foto-eletrônico ou foto-ótico) mostra que se trata de definição para fins estritamente legais, jurídicos, razão pela qual a lei exclui expressamente as modalidades *wire*, *oral* e as transferências eletrônicas de valores depositados em instituições financeiras[163], que, em seus significados tecnológicos, também fariam parte do grupo das *electronic communications*.

Diante disso, o presente capítulo caminha para a conceituação da expressão comunicação telemática em sua acepção exclusivamente jurídica, não havendo razoabilidade em se modificar a interpretação, por exemplo, do significado do que o constituinte pretendeu expressar ao empregar, no artigo 5º, inciso XII, o termo "telefônicas" pelo só fato de que o processo comunicativo sofreu uma mudança. Não faria sentido, igualmente, sustentar que as ligações telefônicas atuais, digitais, passaram a se enquadrar no conceito constitucional de comunicação "de dados".

Será telemática, portanto, em seu sentido jurídico adotado para o presente trabalho, a comunicação que se realize de forma digital, ou seja, que se utilize da conversão em séries binárias, seja qual for a infraestrutura de que se utilize, desde que não se enquadre nas modalidades específicas *telefônica* e *telegráfica*.

Definido o conceito jurídico de interceptação telemática, há que se tratar da chamada rede mundial de computadores, conhecida como internet, por meio da qual se realiza a maior parte das comunicações telemáticas.

---

[162] Nas transmissões digitais de rádio, na verdade, há sempre uma dualidade com a transmissão analógica a qual, inclusive, tem maior alcance, mas menor qualidade de som. Para mais: YOUNKER, Emily. **How Digital Radio Works**. Disponível em: <http://digital-radio-review.toptenreviews.com/how-digital-radio-works.html>. Acesso em: 25 ago. 2013.

[163] USC Section 18 § 2510(12). Ver item 3.1.2, *infra*.

A internet não constitui um meio ou uma infraestrutura de telecomunicações propriamente dita, ou, menos ainda, o conteúdo de coisa alguma, mas sim um sistema que se serve de um meio e de uma infraestrutura para funcionar e transportar conteúdos de informações.

Inicialmente chamada *Arpanet*, a internet foi criada no final dos anos 60 com finalidades exclusivamente militares visando à descentralização das informações, antes concentradas em Washington, para que a comunicação entre os cientistas e engenheiros militares resistisse a um ataque durante a Guerra Fria[164].

No Brasil, a internet chegou em 1988, com acesso restrito às universidades e centros de pesquisa e, após a Portaria nº 295, de 20.07.1995, do Ministério das Telecomunicações, permitiu-se o acesso ao público através das empresas denominadas provedores de acesso[165].

Na internet, a comunicação se dá das formas mais diversas, podendo-se citar as mensagens de um para um, através de correio eletrônico, as mensagens de um para vários, através das listas de correio, as bases de dados de distribuição de mensagens, as comunicações em tempo real (por texto, áudio ou áudio e vídeo), a exemplo do Skype, MSN e VoIP, a utilização remota de computadores, os grupos de notícias e a transferência de arquivos via FTP (*file transfer protocol*)[166].

Portanto, conclui-se que toda comunicação realizada através da internet pode ser classificada de telemática, mas o inverso não é verdadeiro, pois nem todas as comunicações telemáticas se utilizam da internet. Exemplo são os sistemas de comunicação interna de grandes empresas que, sem interligação com a internet, se utilizem apenas da rede interna de computadores.

2.2 Meios modernos de interceptação das comunicações telemáticas

Esclarece-se, de início, que, embora sejam conhecidas as divergências acerca do conceito de interceptação, ao presente trabalho interessa somente a sua concepção como instrumento persecutório do Estado, de modo que consideraremos interceptação um meio de

[164] MORI, 2001, p. 62.
[165] Ibid., p. 62.
[166] LÓPEZ, 2007, p. 34.

obtenção de prova[167] promovido por um terceiro (o Estado), que interfere na comunicação travada pelos interlocutores, sem o conhecimento destes[168].

Avançando-se no conceito, tem-se que a interceptação, diferentemente da obtenção de dados que repousem em servidores, constitui a captação de uma comunicação contemporânea, ou seja, que esteja ocorrendo no momento em que for captada[169].

2.2.1 As *backdoors* e a cooptação das maiores empresas da internet pelas agências de inteligência

A interceptação de uma comunicação depende de duas tarefas elementares, quais sejam, coletar e decodificar[170].

A facilidade da primeira, ao menos no caso dos aparelhos móveis, se deve ao "meio" pelo qual as transmissões acontecem, o ar, que, simplesmente, é público, compartilhado[171].

Afinal, se as ondas comunicativas transitam pelo ar, basta captá-las, por meio do equipamento receptor adequado. Quando não há desvio do fluxo para algum órgão de investigação promovido pela operadora de telefonia ou provedor de internet, a captação pode ser feita por equipamento que faça as vezes da torre de comunicação ou estação rádio base (ERB).

Também chamada de *cell site*, a ERB vem a ser a estação fixa com a qual os terminais móveis se comunicam:

---

[167] Ver item 1.7, *supra*.

[168] É o que Antonio Scarance Fernandes chamou de interceptação em sentido estrito (FERNANDES, 2010, p. 92). Para ver outras definições, GOMES; CERVINI, 1997, p. 95/96; BADARÓ, Gustavo Henrique Righi Ivahy. Interceptação de comunicações telefônicas e telemáticas: limites ante o avanço da tecnologia. In: LIMA, Joel Corrêa de; CASARA, Rubens R. R. (Coord.) **Temas para uma perspectiva crítica do direito**: homenagem ao Professor Geraldo Prado. Rio de Janeiro: Lumen Juris, 2010 p. 484.

[169] Nos itens 3.1.4, 3.2.6 e 4.11, abordaremos a distinção entre o tratamento jurídico dado ao acesso estatal aos conteúdos comunicativos que estejam armazenados ou perenizados em bancos de dados e aquele destinado às comunicações captadas no momento em que elas estiverem ocorrendo.

[170] ROHR, Altieres. Entenda como funcionam os grampos de celular. **G1**. 14 abr. 2012. Disponível em: <http://g1.globo.com/platb/seguranca-digital/2012/04/14/entenda-como-funcionam-os-grampos-de-celular/>. Acesso em: 29 set. 2013.

[171] HOW to prevent mobile phone spying. SearchSecurity.com. Coluna Ask the Expert. Disponível em: <http://searchsecurity.techtarget.com/answer/How-to-prevent-mobile-phone-spying>. Acesso em 30 set. 2013.

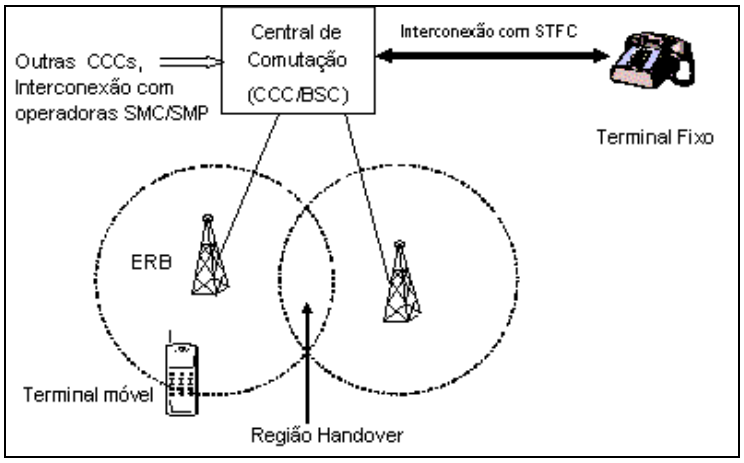

Figura 1 - Ilustração demonstrando o funcionamento das ERBs[172]

A ERB está conectada a uma central de comutação e controle (CCC) que tem interconexão com o serviço telefônico fixo comutado (STFC) e a outras CCCs, permitindo chamadas entre os terminais celulares e deles com os telefones fixos comuns. São também as ERBs que possibilitam a localização de usuários de telefonia móvel através da chamada triangulação dos sinais trocados entre o aparelho e cada uma das estações que se encontrem ao seu redor[173].

Quanto à segunda tarefa, a de decodificar, a situação é bem distinta. Se noutros tempos, quando as transmissões de sinais de telefonia celular eram analógicas, o monitoramento era bastante fácil, na conjuntura atual, após a digitalização das redes, tornou-se muito mais difícil converter ondas eventualmente capturadas para a sua forma original, reveladora de seu conteúdo humano (áudio, texto, imagens, arquivos informáticos). Isto se deve também a uma criptografia inerente às comunicações digitais. Por outro lado, junto com a digitalização das redes, as companhias de telecomunicações e os governos adquiriram formas muito mais fáceis de espionar comunicações[174].

A partir dos documentos de Snowden, o inglês *The Guardian*[175] revelou que agências de inteligência adotaram uma bateria de métodos em sua atuação para superar aquilo que elas enxergam como uma das maiores ameaças à sua capacidade de acessar comunicações, a saber,

---

[172] Disponível em: <http://www.teleco.com.br/tutoriais/tutorialerb/pagina_1.asp>. Acesso em: 13 out. 2013.
[173] Ibid.
[174] HOW to prevent mobile phone spying. SearchSecurity.com. Coluna Ask the Expert. Disponível em: <http://searchsecurity.techtarget.com/answer/How-to-prevent-mobile-phone-spying>. Acesso em 30 set. 2013.
[175] LEWIS, Paul. You're being watched: there's one CCTV camera for every 32 people in UK, **The Guardian**. 02 mar. 2011. Disponível em: <http://www.guardian.co.uk/uk/2011/mar/02/cctv-cameras-watching-surveillance>. Acesso em: 28 jun. 2013.

o uso de criptografia, onipresente em toda a internet. Esses métodos incluem medidas para assegurar o controle da *National Security Agency* (NSA) norte-americana sobre os padrões internacionais de criptografia, o uso de supercomputadores para violar criptografias e o mais bem guardado de todos os segredos, a colaboração das empresas desenvolvedoras de tecnologia e dos próprios provedores de serviços de internet. Foi por meio desta parceria secreta que as agências inseriram nos sistemas comerciais de criptografia, que perante o mercado se anunciam seguros e confiáveis, vulnerabilidades propositais e secretas conhecidas como *backdoors* ou *trapdoors*[176].

Segundo o jornal *The New York Times*, a NSA manteria, graças a este mecanismo subreptício, um banco de dados interno com as chaves para decifrar produtos comerciais específicos, sob o nome de *Key Provisioning Service*, capaz de decodificar automaticamente muitas mensagens[177].

No entanto, a inserção dessas *backdoors* conflita diretamente com a segurança que se pretende para as comunicações mundiais, pois este mecanismo intencional de vulnerabilidade acaba por expor todos os usuários dos sistemas com *backdoors*, e não apenas os alvos das agências de inteligência. Isto porque, segundo Christopher Soghoian, principal tecnologista e analista político diretor da *American Civil Liberties Union*, a inserção de *backdoors* num software aumenta significativamente a dificuldade de se desenvolver um produto seguro[178].

Apesar da atualidade do escândalo midiático provocado por Snowden, já em 1994 o *Communications Assistance for Law Enforcement Act*[179] passou a impor aos operadores de telecomunicações e fabricantes de equipamentos nos Estados Unidos que a concepção de seus

---

[176] Em tradução livre, respectivamente, "porta dos fundos" e "alçapão".

[177] PERLROTH, Nicole; LARSON, Jeff; SHANE, Scott. N.S.A. Able to Foil Basic Safeguards of Privacy on Web. **The New York Times**. 05 set. 2013. Disponível em: <http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=all&_r=0>. Acesso em 27 set. 2013.

[178] LEWIS, Paul. You're being watched: there's one CCTV camera for every 32 people in UK, **The Guardian**. 02 mar. 2011. Disponível em: <http://www.guardian.co.uk/uk/2011/mar/02/cctv-cameras-watching-surveillance>. Acesso em: 28 jun. 2013.

[179] USC Title 47 § 1002 - Assistance capability requirements (a) Capability requirements. Except as provided in subsections (b), (c), and (d) of this section and sections 1007 (a) and 1008 (b) and (d) of this title, a telecommunications carrier shall ensure that its equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of— **(1)** expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to intercept, to the exclusion of any other communications, all wire and electronic communications carried by the carrier within a service area to or from equipment, facilities, or services of a subscriber of such carrier concurrently with their transmission to or from the subscriber's equipment, facility, or service, or at such later time as may be acceptable to the government (Disponível em: <http://www.law.cornell.edu/uscode/text/47/1002>. Acesso em: 02 fev. 2013.

produtos incluíssem mecanismos neles secretamente inseridos de modo a viabilizar o acesso às comunicações telefônicas e de internet em tempo real pelas agências federais[180].

Foi graças à existência dos mecanismos acima, por exemplo, que o FBI implementou seu sistema de monitoramento, o *Digital Collection System Network* (DCSNet), que é mais infiltrado nos sistemas das companhias telefônicas do que se imagina. Dentre suas possibilidades, o DCSNet intercepta linhas de telefonia fixa, linhas de telefone celular, SMS e rádios do tipo *push-to-talk*[181], bem como capta, filtra e armazena números, ligações e mensagens de texto, fornece a localização aproximada do alvo em tempo real através de informações das torres de telefonia celular e desvia o fluxo da interceptação para vans de interceptação (*mobile surveillance vans*)[182].

As funções acima não parecem destoar em muito do brasileiro Guardião, desenvolvido pela empresa catarinense Dígitro e largamente utilizado pelas polícias civis e Federal[183].

Retomando as revelações de Snowden, os documentos vazados mostraram que a NSA destina 250 milhões de dólares por ano a um programa voltado para atuar junto às companhias de tecnologia de modo a promover uma influência secreta sobre o desenvolvimento dos seus produtos[184].

Além disso, como os desenvolvedores de criptografias são altamente dependentes dos padrões definidos mundialmente pelo NIST (*National Institute of Standards and Technology*)[185], órgão com função semelhante à da ABNT brasileira, ligado ao *United States Department of Commerce*, a NSA, desde 2006, introduziu vulnerabilidades, não só nos aplicativos comerciais, mas também nos padrões adotados pelo Instituto[186], o que amplia ainda mais sua capacidade de decifração.

O *Government Communications Headquarters* (GCHQ), equivalente da NSA na Inglaterra, possui, segundo os documentos, um programa voltado para derrubar qualquer obstáculo de criptografia utilizado nos provedores classificados como "*the big four*", a saber,

---

[180] HOW to prevent mobile phone spying. SearchSecurity.com. Coluna Ask the Expert. Disponível em: <http://searchsecurity.techtarget.com/answer/How-to-prevent-mobile-phone-spying>. Acesso em 30 set. 2013.
[181] No Brasil, os rádios *push-to-talk* foram inicialmente oferecidos pela empresa Nextel.
[182] SINGEL, Ryan. Point, Click ... Eavesdrop: How the FBI Wiretap Net Operates. **Wired Magazine.** 29 ago. 2007. Disponível em: <http://www.wired.com/politics/security/news/2007/08/wiretap?currentPage=all>. Acesso em: 02 fev. 2013.
[183] DÍGITRO. Disponível em: <http://www.digitro.com.br/pt/>. Acesso em: 26 ago. 2013.
[184] LEWIS, Paul. You're being watched: there's one CCTV camera for every 32 people in UK, **The Guardian**. 02 mar. 2011. Disponível em: <http://www.guardian.co.uk/uk/2011/mar/02/cctv-cameras-watching-surveillance>. Acesso em: 28 jun. 2013.
[185] GREEN, Matthew. On the NSA. **A Few Thoughts on Cryptographic Engineering** (blog). 05 set. 2013. Disponível em: <http://blog.cryptographyengineering.com/2013/09/on-nsa.html>. Acesso em: 25 set. 2013.
[186] BUCHANAN, Matt. How the N.S.A. Cracked the Web. **The New Yorker**. 07 set. 2013. Disponível em: <http://www.newyorker.com/online/blogs/elements/2013/09/the-nsa-versus-encryption.html>. Acesso em: 06 ago. 2013.

Yahoo, Hotmail, Google e Facebook. Referida agência inglesa teria uma equipe responsável por identificar e recrutar agentes secretos na indústria mundial de telecomunicações[187].

No material, localizou-se uma comunicação entre agências de inteligência comemorando seu sucesso em "*defeating network security and privacy*", ou, em tradução livre, derrotar a segurança e a privacidade da rede. Observou-se, também, uma afirmação da GCHQ de que a inserção de vulnerabilidades nos sistemas comerciais de criptografia seria de conhecimento da NSA, mas somente dela e de ninguém mais, incluindo os clientes comuns, referidos no documento como os "*adversaries*"[188].

Veio à tona, ainda, que a Microsoft colaborou com a NSA para burlar a criptografia no e-mail *Outlook.com* e em serviços de bate-papo, tendo a empresa alegado que foi obrigada a cumprir "exigências legais existentes ou futuras" ao projetar seus produtos. Revelou-se que a Agência adquiriu, ainda, a capacidade de espionar protocolos "seguros" largamente utilizados em todo o mundo, como o *https*, o VoIP (*voice over IP*[189]) e o SSL (*secure sockets layer*), utilizados para proteger compras e operações bancárias on-line[190].

Dentre os objetivos da NSA revelados nos documentos estaria o de adquirir, ainda no ano de 2013, acesso livre de criptografia ao maior serviço de comunicação de áudio e texto da internet, prestado por um grande e não nominado aplicativo que funciona a base de *peer-to-peer*[191]. Pelas descrições, analistas acreditam tratar-se do Skype, hoje pertencente à Microsoft, referida pela NSA nos documentos como "parceira"[192].

---

[187] LEWIS, Paul. You're being watched: there's one CCTV camera for every 32 people in UK, **The Guardian**. 02 mar. 2011. Disponível em: <http://www.guardian.co.uk/uk/2011/mar/02/cctv-cameras-watching-surveillance>. Acesso em: 28 jun. 2013.

[188] LEWIS, Paul. You're being watched: there's one CCTV camera for every 32 people in UK, **The Guardian**. 02 mar. 2011. Disponível em: <http://www.guardian.co.uk/uk/2011/mar/02/cctv-cameras-watching-surveillance>. Acesso em: 28 jun. 2013.

[189] Endereço de IP (*IP address*) é como um número de telefone pessoal para a internet, consistente num número serial que identifica computadores numa rede, podendo, portanto, ser usado para determinar a localização de um equipamento ou a origem de uma mensagem transmitida via internet (IP-ADRESS.COM. Produced by Paul Internet. Homburg, Germany. Disponível em: <http://www.ip-adress.com/>. Acesso em: 03 set. 2013). Um IP é sempre único, pois é a única forma pela qual os sistemas operacionais e dispositivos da rede poderão identificar cada computador, adaptador de rede ou outro equipamento conectado à internet (JORDÃO, Fabio. 2009. **O que é IP estático? E dinâmico?**. 2009. Disponível em: <http://www.tecmundo.com.br/1836-o-que-e-ip-estatico-e-dinamico-.htm>. Acesso em: 02 set. 2013). Exemplos de IP são: 207.169.222.45 (IP *version* 4) e 1234:5678:9000:0D0D:0000:5678:9ABC:8777 (IP *version* 6) (WIRELESS Dictionary. Disponível em: <http://www.wirelessdictionary.com/aw_dictionary_widget_wireless.asp>. Acesso em: 05 set. 2013).

[190] BALL, James; BORGER, Julian; GREENWALD, Glenn. Revealed: how US and UK spy agencies defeat internet privacy and security. **The Guardian**. 06 set. 2013. Disponível em: <http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>. Acesso em: 29 set. 2013.

[191] *Peer to peer*, P2P ou ponto-a-ponto é o tipo de comunicação destinada à troca de informações entre dois equipamentos ou sistemas que são ambos capazes de operar como servidor e cliente. (Tradução livre do autor) (Disponível em: <http://www.wirelessdictionary.com/aw_dictionary_widget_wireless.asp>. Acesso em: 02 nov. 2013); O P2P "difere da rede cliente/servidor convencional porque seus métodos envolvem sistemas servindo outros sistemas. Em redes P2P cada estação possui as mesmas capacidades e responsabilidades." (DURANTE,

Tal "parceria", firmada entre Microsoft e NSA, é confirmada por reportagem de junho de 2013 do *The Washington Post*, que trouxe a público a existência de um sistema secreto utilizado pela NSA e pelo FBI chamado PRISM. A grande novidade é que não se trata de um aplicativo voltado para apenas gerenciar interceptações de comunicações individuais, como o já mencionado DCSNet ou o brasileiro Guardião, mas sim para monitorar diretamente dentro dos servidores das nove maiores empresas americanas de internet, deles extraindo áudio, vídeo, fotos, e-mails, documentos e registros de conexões[193]. A proposta do sistema PRISM, pelo menos a que foi apresentada como justificativa pública para a sua criação, foi a interceptação das comunicações de alvos estrangeiros que, em sua maioria, passam por servidores localizados nos Estados Unidos, mesmo quando remetente e destinatário estejam localizados em outro país[194].

Acrescenta a reportagem que, até 2004, as interceptações promovidas pelo governo americano eram autorizadas relativamente a indivíduos específicos. Entre 2004 e 2007, advogados do governo Bush convenceram o Judiciário a expedir quatro ordens, fundamentalmente novas, até hoje mantidas em sigilo, autorizando o monitoramento maciço de dados[195].

Quanto ao aplicativo Skype, o *The Washington Post* teve acesso a um manual para captação de comunicações via Skype através do PRISM, o chamado "*User's Guide for PRISM Skype Collection*", que orienta o usuário no monitoramento de conversa de áudio e de combinação de áudio, vídeo, chat e transferência de arquivos[196].

Uma apresentação secreta em forma de *slides* revela a possibilidade de acesso aos servidores da *Microsoft* (incluindo o Hotmail e o MSN), Google (incluindo o Gmail), Yahoo, Facebook, Youtube, Skype e Apple:

Gabriel Barros. **Redes Peer-to-Peer**. Universidade Federal do Rio de Janeiro. Departamento de Engenharia Eletrônica e de Computação Disciplina: Redes de Computadores I. Professor: Otto Carlos M. B. Duarte. Disponível em: <http://www.gta.ufrj.br/grad/04_1/p2p/>. Acesso em: 02 out. 2013); São "processos de criptografia que são totalmente realizados nos computadores remetentes e receptores, sem que seja necessário usar nenhum servidor externo" (BUCHSBAUM, Paulo Eduardo Laurenz. **Texto de Criptografia e "Tim Tim"** [mensagem pessoal]. Mensagem recebida por <sidi@ffernandes.adv.br> em 29 set. 2013).

[192] BUCHANAN, Matt. How the N.S.A. Cracked the Web. **The New Yorker**. 07 set. 2013. Disponível em: <http://www.newyorker.com/online/blogs/elements/2013/09/the-nsa-versus-encryption.html>. Acesso em: 06 ago. 2013.

[193] GELLMAN, Barton; POITRAS, Laura. U.S., British intelligence mining data from nine U.S. internet companies in broad secret program. **The Washington Post**. 06 jun. 2013. Disponível em: <http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html>. Acesso em: 15 set. 2013.

[194] Ibid.

[195] Ibid.

[196] Id., Disponível em: <http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_3.html>. Acesso em: 15 set. 2013.

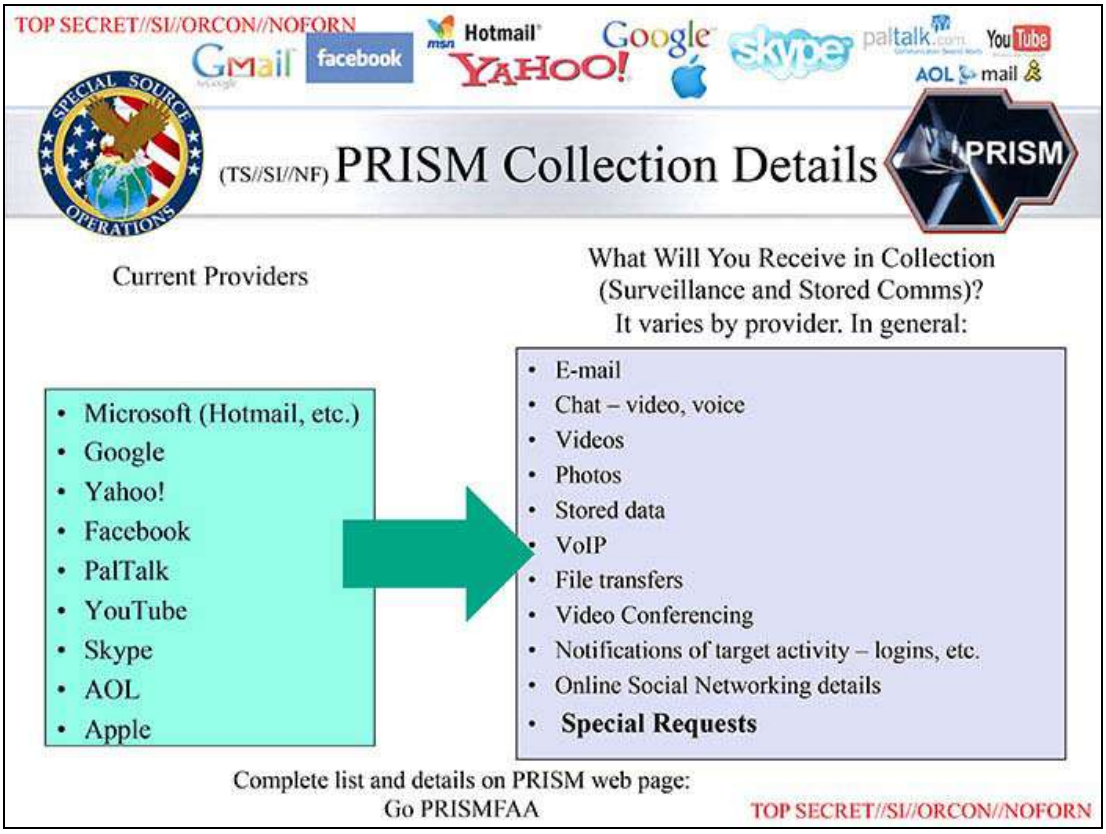

Figura 2 – Apresentação em forma de slides localizada entre os documentos revelados por Edward Snowden demonstrando a capacidade do sistema PRISM[197]

Outro slide[198] revela as datas em que cada empresa aderiu ou, noutras palavras, viabilizou o acesso do PRISM a seus servidores através de *backdoors*:

[197] GELLMAN, Barton; POITRAS, Laura. U.S., British intelligence mining data from nine U.S. internet companies in broad secret program. **The Washington Post**. 06 jun. 2013. Disponível em: <http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/>. Acesso em: 15 set. 2013.

[198] GELLMAN, Barton; POITRAS, Laura. U.S., British intelligence mining data from nine U.S. internet companies in broad secret program. **The Washington Post**. 06 jun. 2013. Disponível em: <http://www.washingtonpost.com/posttv/video/thefold/nsa-leak-source-believes-exposure-consequences-inevitable/2013/06/07/fb15c0fe-cf94-11e2-8845-d970ccb04497_video.html>. Acesso em: 15 set. 2013.

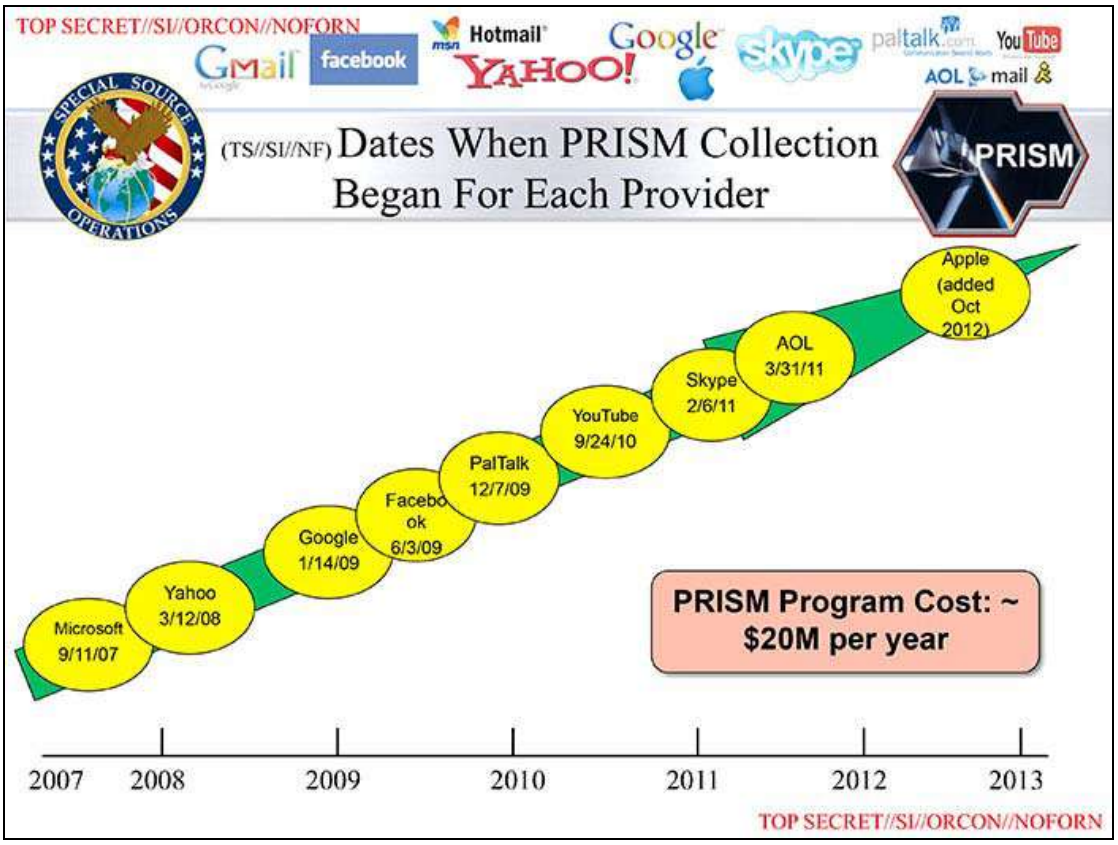

Figura 3 – Slide indicando as datas em que cada empresa aderiu ao programa PRISM[199]

Voltando aos métodos sub-reptícios de inserção de *backdoors*, verificou-se, também, um caso em que o governo americano, ao tomar conhecimento de que um alvo estrangeiro encomendou um novo hardware voltado para comunicações, convenceu o fabricante a inserir uma *backdoor* no produto antes de remetê-lo ao cliente[200].

Após o escândalo Snowden, a justificativa do governo americano ao mundo foi no sentido de que a capacidade de violar criptografias é vital para suas missões fundamentais de contraterrorismo e monitoramento de inteligência estrangeira.

No entanto, episódios posteriores já revelaram que a espionagem excedeu em muito os declarados interesses na persecução ao terrorismo, como foi o caso da espionagem realizada

[199] GELLMAN, Barton; POITRAS, Laura. U.S., British intelligence mining data from nine U.S. internet companies in broad secret program. **The Washington Post**. 06 jun. 2013. Disponível em: <http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/>. Acesso em: 15 set. 2013.

[200] PERLROTH, Nicole; LARSON, Jeff; SHANE, Scott. N.S.A. Able to Foil Basic Safeguards of Privacy on Web. **The New York Times**. 05 set. 2013. Disponível em: <http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=all&_r=0>. Acesso em 27 set. 2013: "In one case, after the government learned that a foreign intelligence target had ordered new computer hardware, the American manufacturer agreed to insert a back door into the product before it was shipped, someone familiar with the request told The Times."

na empresa brasileira Petrobras, o que ensejou a declaração da Presidente Dilma Roussef, no discurso de abertura da 68ª Assembleia Geral da ONU, no sentido de que "não se sustentam argumentos de que a interceptação ilegal de informações e dados destina-se a proteger as nações contra o terrorismo"[201].

2.2.2 Aplicativos especialmente voltados para a criptografia

Como se viu acima, a telefonia celular digital conta com uma criptografia embutida nos protocolos GSM e CDMA[202], mas que já é antiga e hoje facilmente decifrável até mesmo por equipamentos portáteis que captam o sinal, processam e o decodificam[203].

Também as comunicações telemáticas ostentam um nível básico de criptografia que já lhes é inerente (e-mail, Skype, MSN etc.), mas que, sem a colaboração do fabricante no sentido de instalação de uma *backdoor*, acaba por dificultar a decifração dos dados. Não que seja impossível a violação forçada da criptografia, mas a tarefa demandaria dias ou meses de trabalho de supercomputadores[204], trabalhando simultaneamente, com divisão de tarefas, de modo que o custo do esforço computacional pode não compensar o valor da informação resultante da decodificação[205].

Há no mercado, entretanto, aplicativos cuja própria razão existencial é a impenetrabilidade da criptografia, sendo os mais eficientes aqueles funcionando a base de

---

[201] ESPIONAGEM é afronta, diz Dilma na ONU: Na abertura da 68ª Assembleia Geral presidenta ressaltou que interceptações ferem o direito internacional e a soberania dos países. **Carta Capital**. 24 set. 2013. Disponível em: <http://www.cartacapital.com.br/politica/201cjamais-pode-uma-soberania-firmar-se-em-detrimento-de-outra201d-diz-dilma-sobre-espionagem-6642.html>. Acesso em: 30 set. 2013.

[202] GSM (Special Mobile Group) é um padrão globalmente aceito para comunicação celular digital criado pela Conference of European Postal And Telecommunications Administrations (CEPT). CDMA (Code Division Multiple Access) é um canal de rádio compartilhado por múltiplos usuários através do qual se utiliza um único código para cada sinal transmitido ou recebido de cada aparelho (WIRELESS Dictionary. Disponível em: <http://www.wirelessdictionary.com/>. Acesso em: 05 set. 2013). No sistema CDMA, tanto os dados, quanto a voz são transmitidos em um amplo conjunto de frequências, de modo que sobre mais espaço para a transferência de dados (CLUBE DO HARDWARE. Desenvolvido por Gabriel Torres. Disponível em: <http://www.clubedohardware.com.br/artigos/Que-tecnologia-e-melhor-GSM-ou-CDMA/104>. Acesso em: 25 ago. 2013).

[203] BUCHSBAUM, Paulo Eduardo Laurenz. **Texto de Criptografia e "Tim Tim"** [mensagem pessoal]. Mensagem recebida por <sidi@ffernandes.adv.br> em 29 set. 2013.

[204] Atualmente, o mais poderoso supercomputador do mundo é o chinês Tianhe-2, capaz de realizar 34 quatrilhões de cálculos matemáticos por segundo (GREGO, Maur. O mais poderoso supercomputador do mundo agora é chinês. **Revista Exame**. 17 jun. 2013. Disponível em: <http://exame.abril.com.br/tecnologia/noticias/o-mais-poderoso-supercomputador-do-mundo-agora-e-chines>. Acesso em 23 set. 2013.

[205] BUCHSBAUM, Paulo Eduardo Laurenz. **Texto de Criptografia e "Tim Tim"** [mensagem pessoal]. Mensagem recebida por <sidi@ffernandes.adv.br> em 29 set. 2013.

peer-to-peer ou ponto-a-ponto, ou seja, processos de criptografia totalmente realizados, respectivamente, nos computadores remetentes e receptores, sem a necessidade de contar com um servidor externo[206].

Segundo reportagem do *site* G1, uma comunicação, para ser imune ao grampo, precisa utilizar a criptografia *peer-to-peer*, tendo em vista que as criptografias já inerentes aos aplicativos populares proporcionam o embaralhamento dos dados apenas em parte do trajeto da comunicação. Mais precisamente, as comunicações realizadas através dos aplicativos tradicionais saem de um usuário remetente para um destinatário, porém passando, antes, num servidor, onde os dados são desembaralhados ao chegar e novamente embaralhados ao seguir para o destinatário:

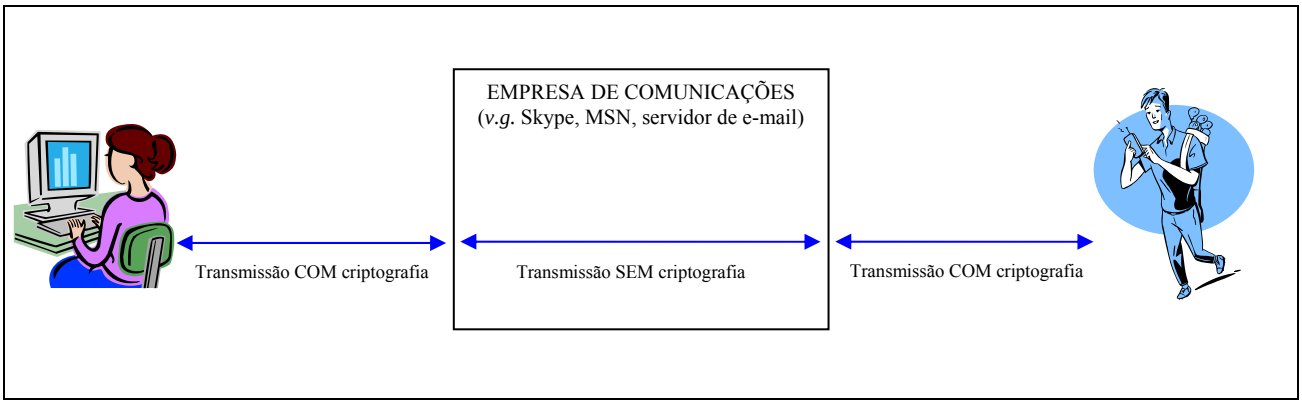

Gráfico 1 – Representação gráfica desenvolvida pelo próprio autor demonstrando os trechos criptografados das comunicações realizadas através de aplicativos.

Portanto, o controlador daquela modalidade comunicativa sempre terá a possibilidade de desviar o fluxo das comunicações de determinado usuário para um órgão estatal de forma totalmente descriptografada ou, naturalmente, com uma criptografia para a qual o órgão possua a chave de acesso.

Diante disso, a referida criptografia *peer-to-peer* se estabelece diretamente entre remetente e destinatário, de modo que só ambos possuam a chave decifradora.

Como dito na introdução do trabalho, o autor, durante a pesquisa, adquiriu um renomado software israelense de criptografia que funciona na modalidade ponto-a-ponto, de

[206] BUCHSBAUM, Paulo Eduardo Laurenz. **Texto de Criptografia e "Tim Tim"** [mensagem pessoal]. Mensagem recebida por <sidi@ffernandes.adv.br> em 29 set. 2013.

modo a enriquecer a pesquisa. Trata-se do aplicativo Gold Lock, que ofereceu um prêmio de 250 mil dólares ao hacker, matemático ou espião que conseguisse violar sua criptografia[207].

Em e-mail trocado entre o autor e o diretor da Gold Lock Brasil, foi perguntado e respondido o seguinte:

> A NSA ou outro órgão dos EUA exige da GL as chaves e interfaces necessárias a interceptar as comunicações via GL?
> Vocês negariam um pedido ou ordem nesse sentido formulado pela Polícia de Israel para investigar terroristas antissionistas ou movimentos iranianos que planejam atacar Israel?
>
> O Gold Lock foi construído e projetado para NÃO permitir *backdoor*, porta dos fundos, portanto o próprio fabricante NÃO tem como entregar chaves, que são geradas randomicamente a cada ligação e depois descartadas.
> Existem diversas outras técnicas e maneira de investigação, que não sejam via escuta telefônica [...][208]

2.2.3 Outros métodos de interceptação: o método *roving bug*, a interceptação de rádios *push-to-talk*, a tecnologia *keyword spotting*, a interceptação integral do fluxo de dados, a busca virtual e os *keyloggers* e *screenloggers*

De início, quanto à idéia de que exista uma capacidade do agente investigador de, remotamente, acionar o microfone de um telefone celular com fins a captar o som do ambiente, apesar de tal medida não constituir uma interceptação telemática, entendemos válido o esclarecimento em razão das dúvidas que a questão gera. A técnica, que, de fato, existe, chama-se *roving bug*, que, numa tradução livre e literal, poderia significar "inseto itinerante". Neste caso, a revelação partiu de uma publicação, em 2006, de Lewis Kaplan, um dos juízes da *Southern District of New York Court*, que apreciou a legalidade da medida[209].

---

[207] PREMIO oferecido de US$250,000: + de 5000 Hackers & Spies Competindo: Não há vencedores: E, francamente, nós não estamos surpresos. GOLD LOCK Gold Line Group Ltd. Disponível em: <https://www.gold-lock.com/pt/hackerchallenge/>. Acesso em: 27 set. 2013.

[208] COPELIOVITCH, Marcelo. **Re: Gold Lock - Secure Call To Any Phone Number** [menssagem pessoal]. Mensagem recebida por sidi@ffernandes.adv.br em 09 set. 2013.

[209] ESTADOS UNIDOS DA AMÉRICA. United States District Court, Southern District of New York. United States of America v. John Tomero et al., No. S2 06 Crim. 0008(LAK). Nov. 27, 2006. Memorandum opinion by Lewis A. Kaplan, District Judge. Disponível em: <http://www.politechbot.com/docs/fbi.ardito.roving.bug.opinion.120106.txt>. Acesso em: 25 set. 2013.

O método foi utilizado pelo FBI para captar conversas pessoais e diretas entre dois membros da família Genovese, talvez a mais famosa e poderosa máfia italiana que já existiu nos Estados Unidos[210].

No momento em que os alvos passaram, cautelarmente, a não mais conversar por telefone, a Corte autorizou a instalação de escutas no restaurante Brunello Trattoria, onde se reuniam. Mas o grupo criminoso localizou o equipamento de escuta, o que deixou seus membros ainda mais cautelosos, passando a fazer reuniões em locais diversificados, prejudicando a investigação. Foi em razão disso que foi pedida e judicialmente autorizada a instalação de equipamento de escuta no aparelho celular do alvo, que captaria o som ambiente, estivesse o aparelho ligado ou desligado[211].

Mas não se compreende com clareza se houve a instalação física de algum artefato no telefone celular do alvo ou se a medida se realizou a distância, pois parece ter havido, no caso Genovese, uma preocupação dos operadores que tomaram conhecimento da técnica investigativa em não divulgar detalhes sobre ela. É o que se vê na petição do Assistant U.S. Attorney Jonathan Kolodner, ao se referir ao equipamento como "meio de escuta colocado no telefone celular", sem se fazer claro se se tratava de um hardware ou software[212].

Considerando, no entanto, que a petição mencionava a Nextel como um provedor de comunicações e o código IMSI[213] de 15 dígitos[214], dados desnecessários para quem pretende instalar um hardware, bem como a dificuldade óbvia de se ter acesso ao aparelho de um alvo tão desconfiado, acredita-se que houve a instalação de um software, a distância e com a colaboração da Nextel.

Analistas de tecnologia asseguram que atualmente a medida é facilmente implementada a distância, mesmo quando os aparelhos estão desligados. Isto porque alguns

---

[210] O lendário chefe da família Genovese era o italiano Vito Genovese, que inspirou o personagem Don Vito Corleone, de Marlon Brando, no filme Godfather (O poderoso chefão).

[211] ESTADOS UNIDOS DA AMÉRICA. United States District Court, Southern District of New York. United States of America v. John Tomero et al., No. S2 06 Crim. 0008(LAK). Nov. 27, 2006. Memorandum opinion by Lewis A. Kaplan, District Judge. Disponível em: <http://www.politechbot.com/docs/fbi.ardito.roving.bug.opinion.120106.txt>. Acesso em: 25 set. 2013.

[212] ESTADOS UNIDOS DA AMÉRICA. United States District Court, Southern District of New York. Application for an order authorizing the interception of oral communications, by Jonathan Kolodner (Assistant United States Attorney). 03 set. 2003. Disponível em: <http://www.politechbot.com/docs/fbi.ardito.affidavit.p1.120106.pdf>. Acesso em: 25 set. 2013.

[213] IMSI (*International Mobile Subscriber Identity*) é um número de identificação atribuído por um prestador de serviço telefônico para identificar um usuário de um telefone móvel (WIRELESS Dictionary. Disponível em: <http://www.wirelessdictionary.com/>. Acesso em: 05 set. 2013). O IMSI está contido no cartão SIM (*subscriber identity module*), que deverá ser inserido nos telefones móveis, sob pena de este não funcionar (TUTORIALSPOINT. Disponível em: <http://www.tutorialspoint.com/>. Acesso em: 30 ago. 2013).

[214] ESTADOS UNIDOS DA AMÉRICA. United States District Court, Southern District of New York. Application for an order authorizing the interception of oral communications, by Jonathan Kolodner (Assistant United States Attorney). 03 set. 2003. Disponível em: <http://www.politechbot.com/docs/fbi.ardito.affidavit.p1.120106.pdf>. Acesso em: 25 set. 2013.

telefones celulares não podem ser completamente desacionados sem que se retire a bateria, como é o caso de alguns modelos da marca Nokia, que, mesmo quando desligados, mantêm ativas algumas funções, a exemplo da de autoacionar o alarme sonoro caso esteja configurado para aquele horário[215].

O correspondente de telecomunicações do *Financial Times* Mark Odell revelou que as operadoras de telefonia podem remotamente instalar um "pedaço de software" em qualquer aparelho móvel, sem o conhecimento do usuário, preparando-o para ativar o microfone mesmo que não haja uma chamada em andamento. Ilustrou a afirmação com a declaração de Sandra Bell, chefe do Departamento de Segurança Interna do Royal United Services Institute, no sentido de que hoje todos nós carregamos inadvertidamente a nossas próprias *carteiras de identidade rastreáveis*, em forma de aparelhos celulares[216].

Artigo publicado pela BBC sobre suspeitas de monitoramento ilegal das comunicações do presidente da ONU e de outros membros de sua diretoria confirma que é comum que sistemas telefônicos possuam *backdoors* que os permitem serem acionados para captar sons do ambiente ainda que o aparelho receptor não esteja ligado no momento, fazendo com que um telefone celular sobre a mesa de político ou empresário se transforme num poderoso e indetectável *bug*[217].

Há registros, também, de um precedente que revelou a capacidade do FBI de acionar remotamente o microfone embutido que existe em alguns sistemas automotivos, como é o caso do *General Motors' OnStar*, e ouvir a conversa dos passageiros sem sua ciência[218].

Passa-se, por fim, a esclarecer outros mitos existentes em torno dos meios modernos de interceptação que aguçam a curiosidade popular[219].

---

[215] MCCULLAGH, Declan; BROACHE, Anne. FBI taps cell phone mic as eavesdropping tool. **CNET News**. 01 dec. 2006. Disponível em: <http://news.cnet.com/2100-1029-6140191.html>. Acesso em: 25 set. 2013.

[216] ODELL, Mark. Use of mobile helped police keep tabs on suspect and brother. **Financial Times**. 02 ago. 2005. Disponível em: < http://cdn.ca9.uscourts.gov/datastore/library/2013/02/26/Oliva_FinancialTimes.pdf>. Acesso em: 29 set. 2013: "If ordered to do so, mobile telephone operators can also tap any calls, but more significantly they can also remotely install a piece of software on to any handset, without the owner's knowledge, which will activate the microphone even when its owner is not making a call, giving security services the perfect bugging device. "We have inadvertently started carrying our own trackable ID card in the form of the mobile phone," said Sandra Bell, head of the homeland security department at the Royal United Services Institute."

[217] WHEELER, Brian. This goes no further... **BBC News Online Magazine**. 02 mar. 2004. Disponível em: <http://news.bbc.co.uk/2/hi/uk_news/magazine/3522137.stm>. Acesso em: 29 set. 2013: "According to one security expert, telephone systems are often fitted with "back doors" enabling them to be activated at a later date to pick up sounds even when the receiver is down. … So provided it is switched on, a mobile sitting on the desk of a politician or businessman can act as a powerful, undetectable bug."

[218] MCCULLAGH, Declan; BROACHE, Anne. FBI taps cell phone mic as eavesdropping tool. **CNET News**. 01 dec. 2006. Disponível em: <http://news.cnet.com/2100-1029-6140191.html>. Acesso em: 25 set. 2013: "Surreptitious activation of built-in microphones by the FBI has been done before. A 2003 lawsuit revealed that the FBI was able to surreptitiously turn on the built-in microphones in automotive systems like General Motors' OnStar to snoop on passengers' conversations. When FBI agents remotely activated the system and were listening in, passengers in the vehicle could not tell that their conversations were being monitored."

Esclarece-se que os rádios *push-to-talk*, no Brasil oferecidos pela empresa Nextel, podem perfeitamente ser interceptados, sem qualquer dificuldade técnica e quem o afirmou foi a própria empresa[220].

A famosa maleta de interceptação, de fato, existe. Trata-se de um equipamento capaz de interceptar comunicações GSM, ao um custo superior a R$ 800.000,00[221].

Quanto ao hollywoodiano escaneador de vozes capaz de identificar, em meio a milhares de diálogos orais captados, determinadas palavras escolhidas pelo interceptador, não resta dúvida de que sua existência é real. E não é preciso ir longe para a obtenção desta confirmação, já que o *site* do própria fabricante do brasileiro Guardião mostra que a versão atual do software possui a chamada tecnologia *keyword spotting*, de localização de palavras em áudios digitalizados[222].

Há, ainda, um método de interceptação bastante poderoso e capaz de lidar com uma das notórias dificuldades de se monitorar cem por cento das comunicações de um indivíduo, que vem a ser o fato de que, atualmente, uma pessoa pode se comunicar por dezenas de "canais" que estão, via de regra, ao seu alcance imediato através da internet. Imaginando um alvo dentro de sua residência pretendendo transmitir uma mensagem a outrem, ele poderá fazê-lo pelo Skype ou MSN de seu computador *desktop*, pelo aplicativos WhatsApp ou BBM de seu telefone móvel ligado à rede *wifi*, por e-mail ou através de muitas outras formas.

Para lidar com isso, diante da dificuldade de se obter a colaboração dos servidores de cada um desses aplicativos, criou-se a chamada interceptação de todo o fluxo de internet, associada a um procedimento chamado busca virtual[223].

Pelo primeiro procedimento, desvia-se cada *byte* de informação enviado e recebido através do cabo de alimentação de internet de uma determinada residência ou empresa. De fato, pelo *link* do provedor (a exemplo de Virtua, Velox, Mundvox etc.) passará cem por cento

---

[219] Reportamo-nos aqui aos esclarecimentos que apresentamos na introdução do presente trabalho no que diz respeito às escassas fontes de pesquisa que subsidiaram o presente capítulo.

[220] ROHR, Altieres. Entenda como funcionam os grampos de celular. **G1**. 14 abr. 2012. Disponível em: <http://g1.globo.com/platb/seguranca-digital/2012/04/14/entenda-como-funcionam-os-grampos-de-celular/>. Acesso em: 29 set. 2013: "Em nota ao G1, a Nextel diz que é possível realizar 'interceptação telefônica de qualquer linha que trafegue em sua área de cobertura, mesmo que habilitada fora do país, por meio de ordem judicial válida, na forma da lei'. A Nextel norte-americana (chamada de Sprint Nextel) tem capacidade para realizar grampos em sistemas de rádio, pelo menos, desde 2002, segundo um documento destinado à polícia norte-americana e que foi publicado na internet pelo site "Cryptome". O documento não faz nenhuma menção a qualquer dificuldade técnica para realizar esse tipo de interceptação."

[221] Exemplar à venda, por R$ 898.000,00, CASA DO DETETIVE. Disponível em: <http://casadodetetive.com.br/interceptor-multiband-dispositivo-decifracao-p-436.lgz?osCsid=a0e9225248672a8937d67220b521bf45>. Acesso em: 23 set. 2013.

[222] DIGITRO. Disponível em: <http://m.digitro.com.br/inteligencia>. Acesso em: 26 ago. 2013.

[223] MALAN, Diogo Rudge. **Interceptação telemática** [mensagem pessoal]. Mensagem recebida por <sidi@ffernandes.adv.br> em 12 nov. 2012.

do que um determinado usuário envia e recebe, seja através de seus computadores *desktop*, seja através dos roteadores *wifi*, excetuando-se, naturalmente, o que transitar pelo serviço de dados da operadora de telefonia móvel (caso o telefone móvel do usuário não esteja se servindo da rede *wifi* do local).

Com isso, o órgão de investigação recebe uma reprodução dos dados trocados por aquele usuário com o mundo externo. Será neste material arrecadado que se realizará o segundo procedimento, de busca virtual, pela qual os investigadores conseguirão isolar as senhas digitadas e contas criadas pelo usuário nos mais diversos servidores. Munidos desses dados, senhas e contas de usuário, o órgão de investigação poderá acessar contas de e-mail, Skype e outros aplicativos. No caso de *webmail*, ou seja, aqueles que são acessados através de *sites*, e não de aplicativos gerenciadores de mensagens (como Outlook), os investigadores poderão ler todas as mensagens enviadas e recebidas e até mesmo marcá-las com o *status* "não lidas" para que o alvo não perceba que está sendo monitorado.

Vale observar que a medida acima é capaz de obter até mesmo as mensagens salvas na pasta de rascunhos. A relevância disso é que salvar mensagens na pasta de rascunho sem, no entanto, enviá-las vem a ser uma inusitada técnica antimonitoramento, consistente na redação de uma mensagem, que poderá conter fotos, áudios, vídeos ou documentos anexados, que será salva, mas não enviada. Em seguida, após um sinal qualquer do remetente ao destinatário, este acessa a conta de e-mail e lê o que está salvo na pasta de rascunho.

Afinal, apesar de tal técnica não demandar envio ou recebimento de mensagem, a aquisição da senha permitirá ao investigador acessar a pasta de rascunho e ler todo o seu conteúdo.

Outro método para se obter senhas é o chamado *keylogger*, que vem a ser um programa, que precisa ser instalado no computador do alvo, que passa a capturar e armazenar todas as teclas digitadas pelo usuário. O artifício dará ao espião não só senhas digitadas, mas números de cartão de crédito e dados digitados em declarações de imposto de renda. Diante disso, algumas instituições bancárias desenvolveram os chamados teclados virtuais, na tela, para dispensar o uso do teclado. Mas contra este método defensivo, já existem os chamados *screenloggers*, capazes de armazenar a posição do cursor e a tela apresentada no monitor[224].

[224] KUROKAWA, Adriana Shimabukuro et al. **Crimes cibernéticos**: manual prático de investigação. São Paulo: Ministério Público Federal, Procuradoria da República do Estado de São Paulo, Grupo de Combate aos Crimes Cibernéticos, 2006, p. 12/13.

2.2.4 Sistemas em uso no Brasil

Como dito na introdução do presente trabalho, as duas empresas fabricantes das principais ferramentas brasileiras de monitoramento, a Dígitro e a Suntech, recusaram-se a fornecer informações ou dados que subsidiassem a pesquisa.

No entanto, a empresa de telefonia Claro disponibilizou em seu *site* um manual do sistema chamado *Suntech Vigia Interception Achievement Suite*[225], que gerencia o monitoramento de mensagens de texto (SMS) e permite a localização do assinante através das ERBs.

Diante disso, ferramentas com as quais o autor até já havia tido um brevíssimo contato, que lhe foi franqueado numa repartição policial, em momento em que se realizava monitoramento de comunicações, poderão dar ao trabalho a ilustração pretendida:

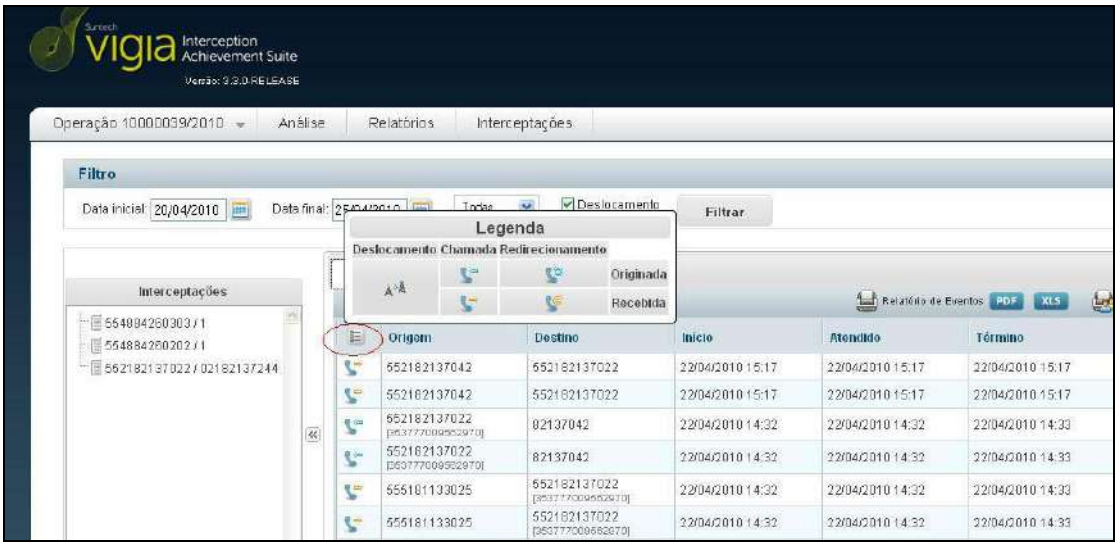

Figura 4 – Tela de gerenciamento de interceptações telefônicas

[225] SUNTECH VIGIA. Interception Achievement Suite. Manual do Usuário Vigia 3. Outubro/2011. Disponível em: https://vigia.claro.com.br/VigiaDadosClient/custom/doc/Manual_VIGIA3_Consulta.pdf;jsessionid=17AC1571FB9CF8BA129C7D3821809BC9.tomcat1. Acesso em: 14.10.2013.

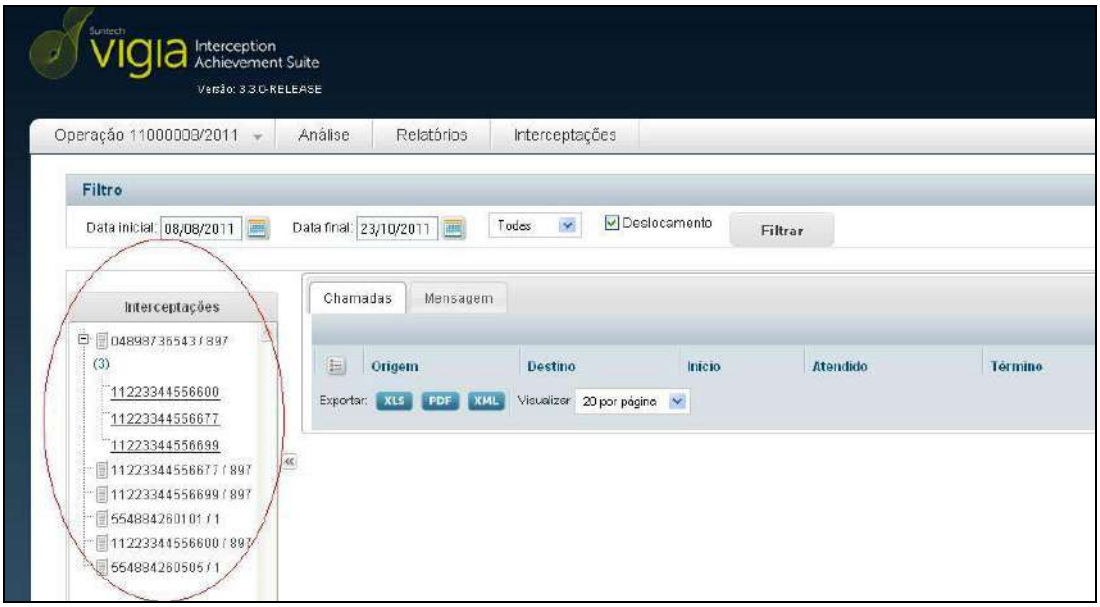

Figura 5 – A figura acima mostra três diferentes IMEIs[226] vinculados a uma mesma linha monitorada, indicando que o usuário utilizou três aparelhos. Trata-se de função que permite ao órgão de investigação, ao identificar os aparelhos já utilizados por um indivíduo, manter o monitoramento, mesmo que o alvo passe a utilizar outro cartão SIM, desde que utilize um daqueles três aparelhos.

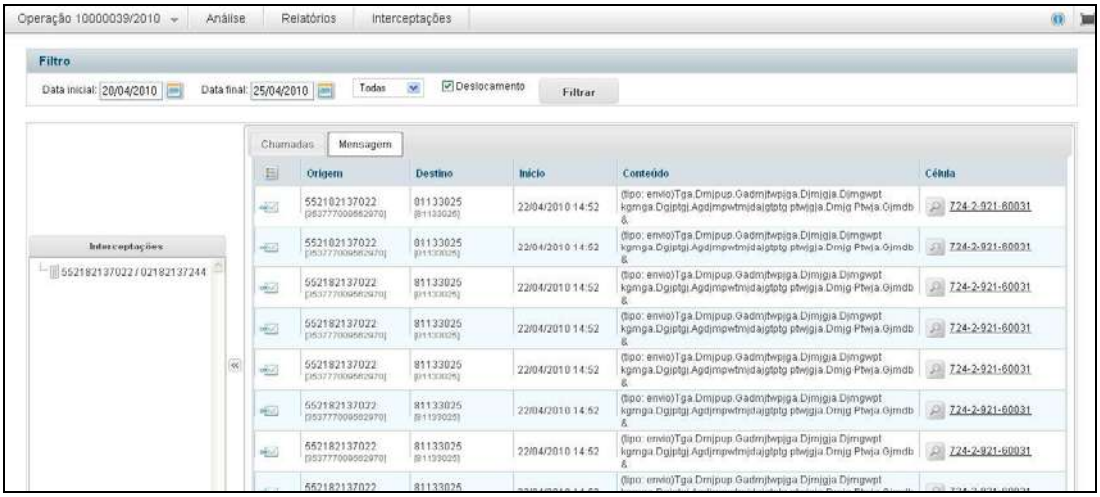

Figura 6 – Tela de gerenciamento de interceptação de mensagens de texto (SMSs). A coluna 'conteúdo' mostra o teor das mensagens trocadas, mas, no quadro acima, estão substituídas por caracteres meramente exemplificativos.

[226] IMEI (*International Mobile Equipment Identifier*) é um número serial de 14 dígitos encontrado em cada aparelho telefônico móvel do tipo GSM (Para a interpretação do significado de cada grupo de dígitos: "Six digits are used for the type approval code (TAC), two digits are used for the final assembly code (FAC), and six digits are used for the serial number. A 16 digit version of the IMEI (IMEI/SV) also contains two digits that are used for the software version number." (WIRELESS DICTIONARY. Disponível em: <http://www.wirelessdictionary.com/Wireless-Dictionary-International-Mobile-Equipment-Identifier-IMEI-Definition.html>. Acesso em: 05 set. 2013).

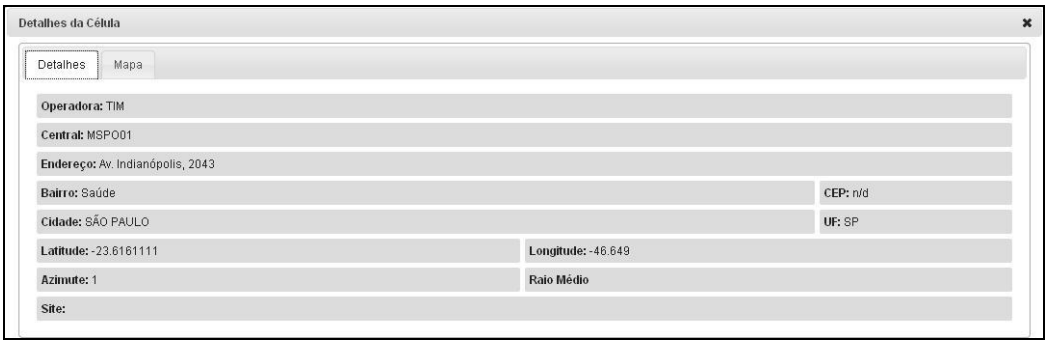

Figura 7 – Tela de localização do assinante através da ERB utilizada pelo aparelho móvel. Os dados acima (endereço, latitude e longitude) se referem à posição da antena, e não do assinante. As informações 'azimute' e 'raio' fornecem ao órgão de investigação uma posição meramente aproximada do aparelho móvel em relação à antena.

Figura 8 – Tela do mapa do sistema Vigia que auxilia na localização de um assinante através da ERB que utilizou. O ícone marrom no meio do mapa indica a posição da antena.

Sobre a localização do assinante por meio das ERBs, a localização rápida de determinado alvo no Brasil, caso se queira, por exemplo, prendê-lo em flagrante por

determinado crime, não é factível devido à baixa precisão dos dados que as companhias telefônicas fornecem aos órgãos de investigação[227].

A informação, no entanto, conflita com notícia publicada no jornal *Financial Times*, que explicou a técnica ao narrar uma investigação realizada nos Estados Unidos. Diz a reportagem que, usando-se apenas três antenas, num processo chamado de triangulação, é possível obter a localização de um indivíduo numa área urbana de alta densidade, com precisão entre dois e três metros, sendo o desvio médio de apenas 25 metros[228].

[227] SILVA JR., José Batista da. **Telemática** [mensagem pessoal]. Mensagem recebida por <sidi@ffernandes.adv.br> em 09 out. 2013.

[228] "As long as the handset is switched on the telephone can be tracked across any mobile network in real time. By using no more than three mobile telephone masts or base stations - a process known as triangulation - it is possible to pin down the location of an individual in high density urban areas to between two and three metres. Crucial to this triangulation is the proximity to each other of the three base stations, but on average the standard deviation is no more than 25 metres." (ODELL, Mark. Use of mobile helped police keep tabs on suspect and brother. **Financial Times**. 02 ago. 2005. Disponível em: <http://cdn.ca9.uscourts.gov/datastore/library/2013/02/26/Oliva_FinancialTimes.pdf>. Acesso em: 29 set. 2013).

3 A INTERCEPTAÇÃO DAS COMUNICAÇÕES TELEMÁTICAS: DIÁLOGOS DE DIREITO COMPARADO

3.1 Estados Unidos da América

3.1.1 A Quarta Emenda e a *expectation of privacy*

Ao tratar da Quarta Emenda à Constituição dos Estados Unidos[229] e da extensão da proteção que deve ser dada à privacidade do indivíduo, a jurisprudência daquele país toma em consideração, como uma espécie de base de raciocínio, o conceito de *expectation of privacy*, consistente na razoabilidade da crença do individuo em que, em determinada circunstância, ninguém, além do(s) interlocutor(es) de sua escolha, poderá conhecer o teor de suas comunicações, sejam aquelas travadas de forma presencial e direta, sejam aquelas que se desenvolvem através de transmissão a distância. E, mais do que se verificar se há ou não *expectation of privacy* em determinadas circunstâncias, ganha relevância a verificação dos níveis de *expectation of privacy* nesta ou naquela situação.

O conceito é bem ilustrado no voto concorrente do Justice Harlan, da Suprema Corte dos Estados Unidos, no caso *Katz v. United States*, em que ele se diz de acordo com a opinião da Corte, no sentido de que uma cabine telefônica, tal qual uma casa, mas diferentemente de um campo aberto, é um espaço em que um indivíduo tem a razoável *expectation of privacy* constitucionalmente protegida. Ainda segundo Harlan, uma invasão eletrônica num espaço privado em tais termos, tal qual uma invasão física, poderia constituir violação à Quarta Emenda, não sendo tais invasões razoáveis se não executadas mediante um mandado judicial[230].

---

[229] Amendment IV - The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized (Disponível em: <http://www.law.cornell.edu/constitution/fourth_amendment>. Acesso em: 13.02.2013).

[230] ESTADOS UNIDOS DA AMÉRICA. Supreme Court of the United States. Katz v. United States. 389 U.S. 347; 88 S. Ct. 507; 19 L. Ed. 2d 576; 1967. Disponível em: <http://www.lexisnexis.com/hottopics/lnacademic/?>. Acesso em: 13 fev. 2013: "MR. JUSTICE HARLAN, concurring. I join the opinion of the Court, which I read to hold only (a) that an enclosed telephone booth is an area where, like a home, *Weeks* v. *United States*, 232 U.S. 383, and unlike a field, *Hester* v. *United States*, 265 U.S. 57, a person has a constitutionally protected reasonable expectation of privacy; (b) that electronic as well as

Desde o julgamento acima, *Katz v. United States*, tornou-se usual nos acórdãos sobre o tema o uso da expressão *Katz test*[231], que seria o teste para verificar se, sob determinada circunstância, o indivíduo teria uma legítima *expectation of privacy* e se, por outro lado, a sociedade estaria preparada para reconhecer aquela expectativa como razoável[232].

No caso *United States v. Larios*, da *United States Court of Appeals for the First Circuit*, outra passagem ressalta a existência de uma razoável *expectation of privacy* relativa à vigilância de áudio instalada num quarto de motel de um investigado que o mantinha como sua residência temporária[233].

Não há *expectation of privacy*, por exemplo, nas comunicações por rádio que possam ser captadas facilmente ou que se destinem ao público, aí incluídas não apenas as transmissões comerciais, mas os sinais de socorro de navios e aeronaves, rádioamador e as interceptações necessárias para se identificar a localização da fonte de tais transmissões[234].

---

physical intrusion into a place that is in this sense private may constitute a violation of the Fourth Amendment; and (c) that the invasion of a constitutionally protected area by federal authorities is, as the Court has long held, presumptively unreasonable in the absence of a search warrant."

[231] ESTADOS UNIDOS DA AMÉRICA. Court of Appeals for the Fifth Circuit. Cressman v. Ellis. 77 Fed. Appx. 744; 2003 U.S. Disponível em: <http://www.lexisnexis.com/hottopics/lnacademic/?>. Acesso em: 13 fev. 2013: "the alleged invasion of the employees' privacy occurred 24 years after the United States Supreme Court established the Katz test for determining whether there had been a violation of privacy."

[232] Assim foi no caso *Smith vs. Maryland*: "(a) Application of the Fourth Amendment depends on whether the person invoking its protection can claim a 'legitimate expectation of privacy' that has been invaded by government action. This inquiry normally embraces two questions: first, whether the individual has exhibited an actual (subjective) expectation of privacy; and second, whether his expectation is one that society is prepared to recognize as 'reasonable.' Katz v. United States, 389 U.S. 347. p. 739/741." (ESTADOS UNIDOS DA AMÉRICA. Supreme Court of the United States. Smith v. Maryland. 442 U.S. 735; 99 S. Ct. 2577; 61 L. Ed. 2d 220; 1979 U.S. Disponível em: <http://www.lexisnexis.com/hottopics/lnacademic/?>. Acesso em: 01 mar. 2013).

[233] ESTADOS UNIDOS DA AMÉRICA. United States Court of Appeals for the First Circuit. United States v. Larios. 593 F.3d 82; 2010 U.S. Disponível em: <http://www.lexisnexis.com/hottopics/lnacademic/?>. Acesso em: 13 fev. 2013: "In United States v. Padilla, 520 F.2d 526 (1st Cir. 1975), we held that secret audio surveillance of a motel room violated the defendant's reasonable expectation of privacy. Id. at 528. Law enforcement agents had rented a motel room for the defendant and installed a hidden microphone in his room. *Id*. at 527. The defendant stayed overnight in the room and used it as his 'temporary residence' while in San Juan, Puerto Rico. *Id*. We concluded that when the defendant was left alone in his room, he had a justifiable expectation of privacy in his surroundings."

[234] STEVENS, Gina Marie; DOYLE, Charles. **Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping**. Congressional Research Service, CRS Report for Congress. Prepared for Members and Committees of Congress, October 9, 2012, p. 14: "Exemptions: Publicly Accessible Radio Communications - Radio communications which can be inadvertently heard or are intended to be heard by the public are likewise exempt. These include not only commercial broadcasts, but ship and aircraft distress signals, tone-only pagers, marine radio and citizen band radio transmissions, and interceptions necessary to identify the source of any transmission, radio or otherwise, disrupting communications satellite broadcasts ('(g) It shall not be unlawful under this chapter or chapter 121 of this title for any person—(i) to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public; (ii) to intercept any radio communication which is transmitted—(I) by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress; (II) by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public; (III) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or (IV) by any marine or aeronautical communications system; (iii) to engage in any

No caso *United States v. Knotts*, de 1983, a Suprema Corte dos Estados Unidos reformou decisão de corte inferior que julgara ilícito o monitoramento e a perseguição de um veículo através de um aparelho *beeper* nele instalado pela polícia. Entendeu a Suprema Corte que tal monitoramento não invadiu nenhuma legítima *expectation of privacy* já que não houve nenhum tipo de busca e apreensão na forma contemplada pela Quarta Emenda, até porque inexiste *expectation of privacy* relativa a movimentos de um carro que circula pelas vias públicas[235].

3.1.2. *Wire, oral* e *electronic communication*

Considerando a multiplicidade de legislações estaduais existentes nos Estados Unidos, optou-se, no presente estudo, por tomar por base a legislação federal, na qual consta a definição de *electronic communication* como sendo a transferência de sinais, texto, imagens, sons, dados ou inteligência de qualquer natureza transmitida, total ou parcialmente, por cabo, rádio ou sistema eletromagnético, fotoeletrônico ou foto-ótico, excluindo-se as *wire*[236] e as *oral communication*[237], bem como os sinais transmitidos para aparelhos *tone-only pagers*[238],

---

conduct which—(I) is prohibited by section 633 of the Communications Act of 1934; or (II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act; (iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or (v) for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted,' 18 U.S.C. 2511(2)(g).)"

[235] ESTADOS UNIDOS DA AMÉRICA. Supreme Court of the United States. United States v. Knotts. 460 U.S. 276; 103 S. Ct. 1081. Disponível em: <http://www.lexisnexis.com/hottopics/lnacademic/?>. Acesso em: 01 mar. 2013: "Monitoring the beeper signals did not invade any legitimate expectation of privacy on respondent's part, and thus there was neither a 'search' nor a 'seizure' within the contemplation of the Fourth Amendment. The beeper surveillance amounted principally to following an automobile on public streets and highways. A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements."

[236] USC § 2510. "Definitions – (1) 'wire communication' means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce" (Disponível em: <http://www.law.cornell.edu/uscode/text/18/2510>. Acesso em: 26 jan. 2013).

[237] USC § 2510. "Definitions …(2) 'oral communication' means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication" (Disponível em: <http://www.law.cornell.edu/uscode/text/18/2510>. Acesso em: 26 jan. 2013).

[238] Os chamados *tone-only pagers*, hoje já praticamente sem uso, são aparelhos que acionam um simples sinal sonoro que visa apenas a informar o usuário de que este deve contatar o provedor do serviço e junto a este verificar o conteúdo de mensagens lá deixadas por seus interlocutores.

os sinais trocados com dispositivos de rastreamento[239] e as informações sobre transferência eletrônica de valores armazenadas por instituições financeiras em sistemas de comunicação utilizados para armazenamento eletrônico e transferência de valores[240].

A leitura atenta das definições legais das três modalidades comunicativas (*oral*, *wire* e *electronic*) mostra que são conceitos claramente anacrônicos, pois há formas comunicativas que são, ao mesmo tempo, abrangidas pelo conceito de *oral*, *wire* e *electronic communication*, sem que haja distinção hierárquica entre os dispositivos. Por exemplo, não se sabe, a partir de uma análise meramente textual, como enquadrar a comunicação oral por *Skype* quando o sinal de internet que o sustenta é veiculado por cabos.

Recorrendo-se à jurisprudência norte-americana, no entanto, consegue-se restringir a abrangência dos três conceitos, podendo-se verificar, por exemplo, que uma comunicação através de um telefone sem fio não é *oral communication*, pois é feita através de ondas de rádio. No precedente *Price v. Turner*, a *United States Court of Appeals for the Ninth Circuit* afirmou que a *oral communication* seria a própria comunicação presencial, e não, como naquele caso concreto, sinais de rádio trocados entre a base e o fone[241].

---

[239] 18 USC § 3117. "Mobile tracking devices … (b) Definition. As used in this section, the term 'tracking device' means an electronic or mechanical device which permits the tracking of the movement of a person or object." (Disponível em: <http://www.law.cornell.edu/uscode/text/18/3117>. Acesso em: 26 jan. 2013).

[240] 18 USC § 2510. "Definitions … (12) 'electronic communication' means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include: (A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device (as defined in section 3117 of this title); or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds" (Disponível em: <http://www.law.cornell.edu/uscode/text/18/2510>. Acesso em: 26 jan. 2013).

[241] ESTADOS UNIDOS DA AMÉRICA. United States Court of Appeals for the Ninth Circuit. Price v. Turner. 260 F.3d 1144, 1147-48 (9th Cir. 2001). Disponível em: <http://www.lexisnexis.com/hottopics/lnacademic/?>. Acesso em: 25 fev. 2013: "When a cordless phone is used, the parties' words travel over the radio waves between the base unit of the phone and its headset. See Askin v. McNulty, 47 F.3d 100, 104 (4th Cir. 1995). Those radio waves can be easily intercepted and overheard by anyone listening on an ordinary radio receiver. *See McKamey v. Roach*, 55 F.3d 1236, 1239-40 (6th Cir. 1995); *United States v. Smith*, 978 F.2d 171, 178-79 (5th Cir. 1992) ('The significant difference between land line telephone conversations and conversations carried out over early versions of cordless phones was the ease with which cordless phone conversations could be intercepted.'). … The 1986 Wiretap Act's exception for cordless telephone communications was contained in the Act's definition of both 'wire communications' and 'electronic communications.' *See* 18 U.S.C.A. § 2510(1), (12)(A) (West 1990). Probably for that reason, Price attempts to maintain that cordless phone conversations are nevertheless protected by the Act as an 'oral communication,' which is defined as 'any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation.' *See* 18 U.S.C.A. § 2510(2) (West 1990). The interpretation urged by Price, however, would render the definition of 'oral communications' inconsistent with the statutory definitions of 'wire' and [*1148] 'electronic' communications. Moreover, an oral communication must be one 'uttered by a person,' and the interception or disclosure of an oral communication must be of the communication itself. *See id.*; *Smith*, 978 F.2d at 175-76. The interception of a cordless phone's radio transmission is not an interception of the oral utterance itself, but of the radio signal produced by the phone's handset and its base unit. Therefore, the interception of a cordless phone transmission cannot be the interception of an oral utterance. This is the precise holding of the Sixth Circuit in *McKamey, see* 55 F.3d at 1239, which we noted has been cited with approval by

Hipótese de *oral communication* seria, por exemplo, a comunicação direta e presencial entre dois ocupantes de um veículo, que, com uma inegável *expectation of privacy*, travariam um diálogo, não através de transmissão de qualquer espécie, mas de ondas sonoras naturais[242].

Em trabalho doutrinário elaborado para o Congresso dos Estados Unidos e suas comissões, Gina Stevens e Charles Doyle simplificaram a distinção da seguinte forma: "*in oversimplified terms ... telephone (wire), face to face (oral), or computer (electronic) communication*"[243].

Segundo os autores, o termo *electronic communications* englobaria transmissão de rádio e dados, mas excluiria transmissões de rádio que possam ser capturadas inocentemente sem grande dificuldade[244].

Portanto, para o presente trabalho, interessa a analisar as *electronic communications*, cujo procedimento para interceptação, aliás, na maioria dos aspectos, é comum ao das modalidades comunicativas *oral* e *wire*.

3.1.3. *Interception of communications* e obtenção de *stored communication*

A interceptação é definida como a aquisição auricular ou de outra natureza do conteúdo de qualquer comunicação, seja ela *wire*, *oral* ou *electronic*, através do uso de qualquer dispositivo eletrônico, mecânico ou de outra natureza[245].

A jurisprudência, no entanto, exige mais para a definição de interceptação. Considera-se interceptação a captação de uma comunicação contemporânea, ou seja, que esteja ocorrendo no momento em que for captada. Assim se decidiu no caso *United States v. Jones*, em que a *United States District Court for the District of Columbia* afirmou que o regime legal

---

the Supreme Court in *Bartnicki, see* 121 S. Ct. at 1759 n.7, and with which we are in full agreement. The district court therefore properly granted summary judgment on Price's federal claim that Turner violated the Wiretap Act, because the Act provided no protection for her cordless calls at the time Turner intercepted them."

[242] CURTIS, George E. **The law of cybercrime and their investigations**. Boca Raton: CRC Press, Taylor and Francis Group, 2012, p. 277: "The communication intercepted here were in-person voice communications, involving no means of transmission except for natural sound waves. Neither party disputes that the occupants of the vehicle reasonably expected that words spoken between them would be private, not subject to interception or transmission. The communication at issue therefore were 'oral communication' within the ambit of statute."

[243] Em tradução livre: "de forma simplificada ... comunicação telefônica (via cabo), comunicação cara-a-cara (oral) e por meio de computador (eletrônica)" (STEVENS; DOYLE, 2012, p. 12).

[244] Ibid., p. 12: "The term 'electronic communications' encompasses radio and data transmissions generally, but excludes certain radio transmissions which can be innocently captured without great difficulty."

[245] 18 USC § 2510. "Definitions … (4) 'intercept' means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." (Disponível em: <http://www.law.cornell.edu/uscode/text/18/2510>. Acesso em: 26 jan. 2013).

existente em torno das interceptações é aplicável à aquisição de comunicações no momento em que elas são transmitidas, e não, como naquele caso concreto (obtenção de mensagens de texto), à apreensão de tais comunicações quando elas repousem em arquivo eletrônico mantido por terceiros[246].

O acesso a um conteúdo comunicativo que esteja armazenado ou perenizado num banco de dados não é considerado interceptação e está regulado por normas distintas, instituídas pelo chamado *Stored Communications Act*. Tal acesso, às chamadas *stored communications*, depende de um mandado judicial que pode ser expedido muito mais facilmente do que uma autorização para interceptação de comunicações. Para se obter um conteúdo comunicativo armazenado, a lei exige apenas que o órgão responsável pela investigação demonstre ao juiz que aquele conteúdo é relevante para uma investigação em andamento[247], ao passo que, para uma interceptação, as exigências, como será abordado a diante, são significativamente maiores.

Noutras palavras, há uma menor proteção legal aos conteúdos de comunicações que repousem em bancos de dados do que de comunicações em andamento.

Para um dado ser considerado *stored communications*, segundo a lei, ele precisa estar armazenado em poder de prestadores de serviço de comunicação eletrônica. No caso *Fannie Garcia v. City of Laredo, Texas*, por exemplo, não se admitiu tratar como *stored*

[246] ESTADOS UNIDOS DA AMÉRICA. United States District Court for the District of Columbia. United States v. Jones. 451 F.Supp.2d 71, 75, D.D.C. 2006. Disponível em: <http://www.lexisnexis.com/hottopics/lnacademic/?>. Acesso em: 17 fev. 2013: "Moreover, while Jones accurately asserts that text messages constitute 'electronic communications' within the meaning of the Wiretap Act (*see* Def.'s Mot. to Suppress Evid. at 5), this assertion gets him nowhere. Courts consistently have held that the Wiretap Act governs only the acquisition of the contents of electronic communications that occur contemporaneous with their transmission, and not -- as is the case here -- the subsequent acquisition of such communications while they are held in electronic storage by third parties. *See, e.g., United States v. Steiger*, 318 F.3d 1039, 1048-49 (11th Cir. 2003) (holding that 'a contemporaneous interception - *i.e.*, an acquisition during 'flight' - is required to implicate the Wiretap Act with respect to electronic communications'); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (holding that 'for [an electronic communication] to be 'intercepted' in violation of the Wiretap Act, it must be acquired during transmission, not while it is in electronic storage'); *Steve Jackson Games, Inc. v. U.S. Secret Serv.*, 36 F.3d 457, 462 (5th Cir. 1994) (analyzing statutory text and legislative history and concluding that "Congress did not intend for 'intercept' to apply to 'electronic communications' when those communications are in 'electronic storage' "); *see also See* Clifford S. Fishman & Anne T. McKenna, *Wiretapping and Eavesdropping* § 2: 5 (West, 2d ed. 1995) ('An interception [of an electronic communication] occurs … only if the contents are acquired as the communication takes place, not if they are acquired while the communications are in storage.')."

[247] 18 USC § 2703. "Required disclosure of customer communications or records. … (d) Requirements for Court Order: A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider." (Disponível em: <http://www.law.cornell.edu/uscode/text/18/2703>. Acesso em: 17 fev. 2013).

communication as mensagens de texto e imagens extraídas de um aparelho de telefone celular por não se tratar de um prestador de serviço de comunicação[248].

O tema foi bem abordado no caso *Konop v. Hawaiian Airlines, Inc*., pela *United States Court of Appeals for the Ninth Circuit*, que afirmou que, apesar de as mensagens eletrônicas, entre sua remessa e seu recebimento, serem armazenadas em vários computadores, o Congresso, claramente, pretendeu dar menor proteção aos conteúdos armazenados do que àqueles que estejam em seu momento de transmissão[249].

---

[248] Esclarece-se que a extração das mensagens e imagens do aparelho celular não se deu através de interceptação, mas de acesso físico ao aparelho. Foi no caso *Fannie Garcia v. City of Laredo*: "In this appeal, Plaintiff-Appellant Fannie Garcia ('Garcia') contends the district court's interpretation of the Stored Communications Act was erroneous. Garcia alleges that the statute applies and protects all text and data stored on her personal cell phone which the Defendants accessed without Garcia's permission. We conclude that the Stored Communications Act, which prohibits accessing without authorization a facility through which an electronic communication service is provided and thereby obtaining access to an electronic communication while it is in electronic storage, does not apply to data stored in a personal cell phone. ... While the SCA does not define the term 'facility,' it does define the terms 'electronic communication service' and 'electronic storage.' The statute defines an 'electronic communication service' ('ECS') as 'any service which provides to users thereof the ability to send or receive wire or electronic communications.' 18 U.S.C. §2510(15) (incorporated by reference in 18 U.S.C. §2711(1) of the SCA). 'Electronic storage' is defined as '(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.' *Id*. §2510(17). Courts have interpreted the statute to apply to providers of a communication service such as telephone companies, internet or e-mail service providers, and bulletin board services. For example, in *Steve Jackson Games, Inc. v. United States Secret Service*, we found that the SCA applied to cover the seizure of a computer used to operate an electronic bulletin board system. 36 F.3d 457, 462-63 (5th Cir. 1994). Other circuits have applied the SCA to internet service providers. *See, e.g., Councilman*, 418 F.3d at 81-82; *Theofel v. Farey-Jones*, 359 F.3d 1066, 1075 (9th Cir. 2004)" (ESTADOS UNIDOS DA AMÉRICA. United States Court of Appeals for the Fifth Circuit. Fannie Garcia v. City of Laredo, Texas. 702 F.3d 788; 2012 U.S. App. LEXIS 25370. Disponível em: <http://www.lexisnexis.com/hottopics/lnacademic/?>. Acesso em: 17 fev. 2013).

[249] ESTADOS UNIDOS DA AMÉRICA. United States Court of Appeals for the Ninth Circuit. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002). Disponível em: <http://www.lexisnexis.com/hottopics/lnacademic/?>. Acesso em: 15 fev. 2013: "We therefore hold that for a website such as Konop's to be 'intercepted' in violation of the Wiretap Act, it must be acquired during transmission, not while it is in electronic storage. The dissent, amici, and several law review articles argue that the term 'intercept' must apply to electronic communications in storage because storage is a necessary incident to the transmission of electronic communications. *See, e.g.*, Akamine, *supra*, at 561-65; Jarrod J. White, *E-Mail@ Work. Com: Employer Monitoring of Employee E-Mail*, 48 Ala. L. Rev. 1079, 1083 (1997). Email and other electronic communications are stored at various junctures in various computers between the time the sender types the message and the recipient reads it. In addition, the transmission time of email is very short because it travels across the wires at the speed of light. It is therefore argued that if the term 'intercept' does not apply to the *en route* storage of electronic communications, the Wiretap Act's prohibition against 'intercepting' electronic communications would have virtually no effect. While this argument is not without appeal, the language and structure of the ECPA demonstrate that Congress considered and rejected this argument. Congress defined 'electronic storage' as 'any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof,' 18 U.S.C. § 2510(17)(A), indicating that Congress understood that electronic storage was an inherent part of electronic communication. Nevertheless, as discussed above, Congress chose to afford stored electronic communications less protection than other forms of communication. This conclusion is consistent with the ordinary meaning of 'intercept,' which is 'to stop, seize, or interrupt in progress or course before arrival.' *Webster's Ninth New Collegiate Dictionary* 630 (1985). More importantly, it is consistent with the structure of the ECPA, which created the SCA for the express purpose of addressing 'access to *stored* … electronic communications and transactional records.' S. Rep. No. 99-541 at 3 (emphasis added). The level of protection provided stored communications under the SCA is considerably less than that provided communications covered by the Wiretap Act. Section 2703(a) of the SCA details the procedures law

Esta inferioridade na proteção legal destinada a mensagens armazenadas e que, inevitavelmente, baixa as barricadas protetoras do sigilo de comunicações eletrônicas, na medida em que seu processo comunicativo, via de regra, depende de sucessivos armazenamentos durante a transmissão entre o remetente e o destinatário, foi criticada por Spencer Cady (2012), da *Drake Law School*, ao observar que o e-mail se tornou uma ferramenta comum através da qual a sociedade moderna comunica pensamentos, sentimentos e ideias e que mereceria uma adequada proteção de privacidade[250].

A controvérsia gira em torno de dar às mensagens armazenadas a proteção da Quarta Emenda constitucional nelas reconhecendo a presença de uma legítima *expectation of privacy* ou, ao contrário, apenas aquela proteção proporcionada pelo *Title* 18, *Section* 2703, do USC, instituída pelo *Stored Communication Act*.

Orin Kerr (2003), professor da *George Washington University Law School*, observa que, uma vez que a Quarta Emenda não protege informações que tenham sido divulgadas a terceiros, a estrutura de funcionamento da internet parece ter sido desenvolvida de modo a não se enquadrar em sua esfera de proteção. Isto porque, na internet, ao pressionar a tecla "enviar", a mensagem é enviada ao provedor de internet do usuário, divulgando-a para ele com instruções para encaminhá-la ao destinatário. Feito isso, o provedor olha para o e-mail, copia-o e envia a cópia através da internet, na qual o conteúdo é visto por muitos outros computadores antes que chegue no provedor do destinatário. Lá chegando, a mensagem fica armazenada aguardando que o destinatário a requisite. Por isso – diz Kerr –, apesar de o e-mail se parecer com uma carta, seu modo de envio se dá muito mais como o de um cartão postal, totalmente exposto. Kerr, ainda em 2003, observava que era cedo para se afirmar que a Quarta Emenda não oferecia proteção às comunicações via internet[251], o que se devia aos

---

enforcement must follow to access the contents of stored electronic communications, but these procedures are considerably less burdensome and less restrictive than those required to obtain a wiretap order under the Wiretap Act. *See Steve Jackson Games*, 36 F.3d at 463. Thus, if Konop's position were correct and acquisition of a stored electronic communication were an interception under the Wiretap Act, the government would have to comply with the more burdensome, more restrictive procedures of the Wiretap Act to do exactly what Congress apparently authorized it to do under the less burdensome procedures of the SCA. Congress could not have intended this result. As the Fifth Circuit recognized in *Steve Jackson Games*, 'it is most unlikely that Congress intended to require law enforcement officers to satisfy the more stringent requirements for an intercept in order to gain access to the contents of stored electronic communications.' *Id.; see also Wesley Coll.*, 974 F. Supp. at 388 (same)."

[250] CADY, Spencer. S. Reconciling privacy with progress: Fourth Amendment protection of e-mail stored with and sent through a third-party internet service provider. **Drake Law Review**, 61 Drake L. Rev. 225, 2012, p. 1.

[251] KERR, Orin S. **Lifting the "fog" of internet surveillance**: How A Suppression Remedy Would Change Computer Crime Law. Public Law and Legal Theory Research Paper No. 057. The George Washington University Law School, 2003: "Why does this matter to internet surveillance? It matters because the basic design of the internet harnesses the disclosure, sharing, and exposure of information to many machines connected to the network. The internet seems almost custom-designed to frustrate claims of broad Fourth Amendment protection: the Fourth Amendment does not protect information that has been disclosed to third-parties, and the internet

ainda raros precedentes jurisprudenciais que se ocuparam da questão. Mas, desde então, a jurisprudência avançou.

Embora sem conter as respostas completas sobre a questão, o caso *United States v. Warshak* se mostrou um embrião rumo à solução da divergência. Proferido pela *United States Court of Appeals for the Sixth Circuit*, o acórdão fixa a controvérsia na aplicabilidade ou não da Quarta Emenda sobre a questão do acesso pelos órgãos de persecução aos conteúdos de e-mails de assinantes armazenados em provedores comerciais. A Corte destaca o aspecto, que considera fundamental, de que a informação é transmitida através de uma rede de comunicações e o de que a Quarta Emenda precisa acompanhar a inexorável marcha do progresso tecnológico, sob pena de suas garantias se esvaziarem. Observou que, se é reconhecida a incidência da Quarta Emenda sobre as comunicações telefônicas e sobre a correspondência epistolar, sabendo-se que, no caso desta última, o remetente também entrega sua carta ou pacote para que circule entre centenas de funcionários dos correios até que chegue ao destinatário, sem que isto ponha em cheque a legítima *expectation of privacy* do indivíduo ou a aceitação pela sociedade daquela *expectation* como razoável, destinar aos e-mails proteção inferior desafiaria o senso comum. Assim, a possibilidade de um terceiro ou intermediário ter acesso ao conteúdo da comunicação não poderia ser suficiente para extinguir a razoável *expectation of privacy*. Os ocupantes de quartos de hotéis têm reconhecida sua legítima *expectation of privacy* mesmo que camareiras possam lá entrar regularmente. Diante disso, a Corte se convenceu de que a possibilidade de acesso rotineiro, seja pelas camareiras de um hotel, seja pelo operador de telefonia, seja pelos funcionários dos correios, seja pelo provedor de internet, não afasta a legítima *expectation of privacy*, a menos, é claro, que o

---

works by disclosing information to third-parties. Consider what happens when an internet user sends an e-mail. By pressing 'send' on the user's e-mail program, the user sends the message to her ISP, disclosing it to the ISP, with instructions to deliver it to the destination. The ISP computer looks at the e-mail, copies it, and then sends a copy across the internet where it is seen by many other computers before it reaches the recipient's ISP. The copy sits on the ISP's server until the recipient requests the e-mail; at that point, the ISP runs off a copy and sends it to the recipient. While the e-mail may seem like a postal mail, it is sent more like a post card, exposed during the course of delivery. Does this mean that the Fourth Amendment offers no protection to internet communications? It's too early to tell. Courts may follow the logic of this syllogism, or they may not. However, courts have already indicated that defendants do not retain Fourth Amendment protection in non-content information such as basic subscriber information. Courts have also declined to find Fourth Amendment protection in the contents of computer usage in the few fairly specific situations that have been litigated (*See Leis*, 225 F.3d at 333; United States v. Butler, 151 F. Supp. 2d 82 (D. Me. 2001); United States v. Simons, 206 F.3d 392 (4th Cir. 2000). *But see* United States v. Maxwell, 45 M.J. 406 (C.A.A.F. 1996).). At least as of the time of this writing, the answer to the question of how much privacy protection the Fourth Amendment guarantees to internet communications appears to be 'not much.' And certainly not enough."

provedor de e-mails tenha expressamente manifestado ao assinante a intenção de auditar, inspecionar e monitorar o conteúdo de seus e-mails[252].

[252] ESTADOS UNIDOS DA AMÉRICA. United States Court of Appeals for the Sixth Circuit. United States v. Warshak. 631 F.3d 266; 2010 U.S. App. Disponível em: <http://www.lexisnexis.com/hottopics/lnacademic/?>. Acesso em: 27 fev. 2013: "Much hinges, therefore, on whether the government is permitted to request that a commercial ISP turn over the contents of a subscriber's emails without triggering the machinery of the Fourth Amendment. In confronting this question, we take note of two bedrock principles. First, the very fact that information is being passed through a communications network is a paramount Fourth Amendment consideration. *See ibid.; United States v. U. S. Dist. Court*, 407 U.S. 297, 313, 92 S. Ct. 2125, 32 L. Ed. 2d 752 (1972) ('[T]he broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards.'). Second, the Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish. *See Kyllo v. United States*, 533 U.S. 27, 34, 121 S. Ct. 2038, 150 L. Ed. 2d 94 (2001) (noting that evolving technology must not be permitted to "erode the privacy guaranteed by the Fourth Amendment'); *see also* Orin S. Kerr, *Applying the Fourth Amendment to the internet: A General Approach*, 62 Stan. L. Rev. 1005, 1007 (2010) (arguing that 'the differences between the facts of physical space and the facts of the internet require courts to identify new Fourth Amendment distinctions to maintain the function of Fourth Amendment rules in an online environment'). With those principles in mind, we begin our analysis by considering the manner in which the Fourth Amendment protects traditional forms of communication. In *Katz*, the Supreme Court was asked to determine how the Fourth Amendment applied in the context of the telephone. There, government agents had affixed an electronic listening device to the exterior of a public phone booth, and had used the device to intercept and record several phone conversations. *See* 389 U.S. at 348. The Supreme Court held that this constituted a search under the Fourth Amendment, *see id.* at 353, notwithstanding the fact that the telephone company had the capacity to monitor and record the calls, *see Smith*, 442 U.S. at 746-47 (Stewart, J., dissenting). In the eyes of the Court, the caller was 'surely entitled to assume that the words he utter[ed] into the mouthpiece w[ould] not be broadcast to the world.' *Katz*, 389 U.S. at 352. The Court's holding in *Katz* has since come to stand for the broad proposition that, in many contexts, the government infringes a reasonable expectation of privacy when it surreptitiously intercepts a telephone call through electronic means. *Smith*, 442 U.S. at 746 (Stewart, J., dissenting) ('[S]ince *Katz*, it has been abundantly clear that telephone conversations are fully protected by the Fourth and Fourteenth Amendments.'). Letters receive similar protection. *See Jacobsen*, 466 U.S. at 114 ('Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy[.]'); *Ex Parte Jackson*, 96 U.S. 727, 733, 24 L. Ed. 877 (1877). While a letter is in the mail, the police may not intercept it and examine its contents unless they first obtain a warrant based on probable cause. *Ibid.* This is true despite the fact that sealed letters are handed over to perhaps dozens of mail carriers, any one of whom could tear open the thin paper envelopes that separate the private words from the world outside. Put another way, trusting a letter to an intermediary does not necessarily defeat a reasonable expectation that the letter will remain private. *See Katz*, 389 U.S. at 351 ('[W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.'). Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection. *See* Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-Mail*, 2008 U. Chi. Legal F. 121, 135 (2008) (recognizing the need to 'eliminate the strangely disparate treatment of mailed and telephonic communications on the one hand and electronic communications on the other'); *City of Ontario v. Quon*, 130 S. Ct. 2619, 2631, 177 L. Ed. 2d 216 (2010) (implying that 'a search of [an individual's] personal e-mail account' would be just as intrusive as 'a wiretap on his home phone line'); *United States v. Forrester*, 512 F.3d 500, 511 (9th Cir. 2008) (holding that '[t]he privacy interests in [mail and email] are identical'). Email is the technological scion of tangible mail, and it plays an indispensable part in the Information Age. … As an initial matter, it must be observed that the mere *ability* of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy. In *Katz*, the Supreme Court found it reasonable to expect privacy during a telephone call despite the ability of an operator to listen in. *See Smith*, 442 U.S. at 746-47 (Stewart, J., dissenting). Similarly, the ability of a rogue mail handler to rip open a letter does not make it unreasonable to assume that sealed mail will remain private on its journey across the country. Therefore, the threat or possibility of access is not decisive when it comes to the reasonableness of an expectation of privacy. … Hotel guests, for example, have a reasonable expectation of privacy in their rooms. *See United States v. Allen*, 106 F.3d 695, 699 (6th Cir. 1997). This is so even though maids routinely enter hotel rooms to replace the towels and tidy the furniture. Similarly, tenants have a legitimate expectation of privacy in their apartments. *See United States v. Washington*, 573 F.3d 279, 284 (6th Cir. 2009). That expectation persists, regardless of the incursions of handymen to fix leaky faucets. Consequently, we are convinced that some degree of routine access is hardly dispositive with respect to the privacy question. Again,

3.1.4. A proteção aos dados de tráfego

Na comunicação entre dois indivíduos, sendo um o emissor da mensagem e outro seu receptor, transmite-se um conteúdo intelectual, que vem a ser o que um interlocutor deseja que chegue ao conhecimento do outro. Trata-se do conteúdo humano de uma comunicação, que pode ser um áudio, um texto, uma imagem etc.

Mas, junto com o teor principal da mensagem, o processo comunicativo gera outras tantas informações atinentes, por exemplo, à 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. Estes são os chamados dados de tráfego ou dados externos ao processo comunicativo.

Em torno dos dados de tráfego, há controvérsia semelhante à tratada no item anterior.

No caso *United States v. Knotts*, a Suprema Corte dos Estados Unidos afastou a legítima *expectation of privacy* sobre o registro dos números discados por um investigado, na medida em que, com o uso do telefone, o investigado assumiu o risco de que a companhia telefônica registrasse os números que discou e os revelasse à polícia. Afinal, observou a Suprema Corte, o equipamento que registra os números discados seria tão simplesmente a versão moderna do operador de telefonia que, antigamente, completava as ligações para os usuários. Diante do argumento do investigado de que somente se, de fato, se tratasse de um operador humano de antigamente seria razoável se afastar a *expectation of privacy*, a Corte replicou que não seria de se admitir um resultado constitucional distinto só porque a companhia telefônica resolveu se automatizar[253].

---

however, we are unwilling to hold that a subscriber agreement will *never* be broad enough to snuff out a reasonable expectation of privacy. As the panel noted in *Warshak I*, if the ISP expresses an intention to 'audit, inspect, and monitor' its subscriber's emails, that might be enough to render an expectation of privacy unreasonable. *See* 490 F.3d at 472-73 (quoting *United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000)). But where, as here, there is no such statement, the ISP's 'control over the [emails] and ability to access them under certain limited circumstances will not be enough to overcome an expectation of privacy.' *Id*. at 473."

[253] ESTADOS UNIDOS DA AMÉRICA. Supreme Court of the United States. United States v. Knotts. 460 U.S. 276; 103 S. Ct. 1081. Disponível em: <http://www.lexisnexis.com/hottopics/lnacademic/?>. Acesso em: 01 mar. 2013: : "This analysis dictates that [Smith] can claim no legitimate expectation of privacy here. When he used his phone, [Smith] voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, [Smith] assumed the risk that the

No mesmo sentido decidiu a Suprema Corte americana no caso *Smith v. Maryland*, quando afirmou que não há *expectation of privacy*, e se houvesse não seria legítima, acerca dos números discados do telefone do investigado, pois ele sabia que a companhia telefônica os armazena para diversas finalidades comerciais, assumindo, portanto, o risco de que a companhia os fornecesse à polícia[254]. No entanto, votos divergentes dos juízes Stewart e Brennan sustentaram que o fato de a companhia telefônica armazenar registros dos números discados é aspecto próprio da natureza das ligações telefônicas e a questão acerca do que a companhia faz ou pode fazer com esses registros não é em nada mais relevante do que aquilo que ela faz ou pode fazer com o próprio conteúdo das conversas que trafegam na linha[255].

No caso *United States v. Appelbaum*, a *United States Court of Appeals for the Fourth Circuit* decidiu que o acesso a registros de comunicações eletrônicas armazenadas, tais como nome, endereço e tempo de inscrição depende da expedição de autorização judicial, com base

---

company would reveal to police the numbers he dialed. The switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber. [Smith] concedes that if he had placed his calls through an operator, he could claim no legitimate expectation of privacy. [Citation omitted.] We are not inclined to hold that a different constitutional result is required because the telephone company has decided to automate."

[254] ESTADOS UNIDOS DA AMÉRICA. Supreme Court of the United States. Smith v. Maryland. 442 U.S. 735; 99 S. Ct. 2577; 61 L. Ed. 2d 220; 1979 U.S. Disponível em: <http://www.lexisnexis.com/hottopics/lnacademic/?>. Acesso em: 01 mar. 2013: "Petitioner in all probability entertained no actual expectation of privacy in the phone numbers he dialed, and even if he did, his expectation was not 'legitimate.' First, it is doubtful that telephone users in general have any expectation of privacy regarding the numbers they dial, since they typically know that they must convey phone numbers to the telephone company and that the company has facilities for recording this information and does in fact record it for various legitimate business purposes. And petitioner did not demonstrate an expectation of privacy merely by using his home phone rather than some other phone, since his conduct, although perhaps calculated to keep the contents of his conversation private, was not calculated to preserve the privacy of the number he dialed. Second, even if petitioner did harbor some subjective expectation of privacy, this expectation was not one that society is prepared to recognize as 'reasonable.' When petitioner voluntarily conveyed numerical information to the phone company and 'exposed' that information to its equipment in the normal course of business, he assumed the risk that the company would reveal the information to the police, cf. United States v. Miller, 425 U.S. 435. p. 741/746."

[255] ESTADOS UNIDOS DA AMÉRICA. Supreme Court of the United States. Smith v. Maryland. 442 U.S. 735; 99 S. Ct. 2577; 61 L. Ed. 2d 220; 1979 U.S. Disponível em: <http://www.lexisnexis.com/hottopics/lnacademic/?>. Acesso em: 01 mar. 2013: "DISSENT: MR. JUSTICE STEWART, with whom MR. JUSTICE BRENNAN joins, dissenting: I am not persuaded that the numbers dialed from a private telephone fall outside the constitutional protection of the Fourth and Fourteenth Amendments. … the Court today says that those safeguards do not extend to the numbers dialed from a private telephone, apparently because when a caller dials a number the digits may be recorded by the telephone company for billing purposes. But that observation no more than describes the basic nature of telephone calls. A telephone call simply cannot be made without the use of telephone company property and without payment to the company for the service. The telephone conversation itself must be electronically transmitted by telephone company equipment, and may be recorded or overheard by the use of other company equipment. Yet we have squarely held that the user of even a public telephone is entitled 'to assume that the words he utters into the mouthpiece will not be broadcast to the world.' *Katz* v. *United States, supra*, at 352. The central question in this case is whether a person who makes telephone calls from his home is entitled to make a similar assumption about the numbers he dials. What the telephone company does or might do with those numbers is no more relevant to this inquiry than it would be in a case involving the conversation itself. It is simply not enough to say, after *Katz*, that there is no legitimate expectation of privacy in the numbers dialed because the caller assumes the risk that the telephone company will disclose them to the police."

no já mencionado *Title* 18 USC §2703, que exige apenas que o órgão responsável pela investigação demonstre ao juiz que aquele conteúdo é relevante para uma investigação em andamento, ou na chamada *Federal Rule of Criminal Procedure* nº 41[256], que permite a expedição de uma ordem de busca e apreensão mediante a identificação de *probable cause*[257] de buscar e apreender prova de crime, proventos do crime, objetos usados no cometimento de crime ou voltados para serem utilizados para cometer crime[258].

[256] Rule 41. "Search and Seizure ... (c) Persons or Property Subject to Search or Seizure. A warrant may be issued for any of the following: (1) evidence of a crime; (2) contraband, fruits of crime, or other items illegally possessed; (3) property designed for use, intended for use, or used in committing a crime; or (4) a person to be arrested or a person who is unlawfully restrained. (d) Obtaining a Warrant. (1) In General. After receiving an affidavit or other information, a magistrate judge—or if authorized by Rule 41(b), a judge of a state court of record—must issue the warrant if there is probable cause to search for and seize a person or property or to install and use a tracking device. … (2) Contents of the Warrant. (A) Warrant to Search for and Seize a Person or Property. Except for a tracking-device warrant, the warrant must identify the person or property to be searched, identify any person or property to be seized, and designate the magistrate judge to whom it must be returned. The warrant must command the officer to: (i) execute the warrant within a specified time no longer than 14 days; (ii) execute the warrant during the daytime, unless the judge for good cause expressly authorizes execution at another time; and (iii) return the warrant to the magistrate judge designated in the warrant. (B) Warrant Seeking Electronically Stored Information. A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review." (Disponível em: <http://www.law.cornell.edu/rules/frcrmp/rule_41#rule_41_e_2_A>. Acesso em: 04 mar. 2013).

[257] Extraída da Quarta Emenda à Constituição dos Estados Unidos ("Amendment IV. The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." (Disponível em: <http://www.law.cornell.edu/constitution/fourth_amendment>. Acesso em: 27 jan. 2012), a expressão *probable cause* é muito utilizada em direito criminal naquele país. Pode-se dizer que *probable cause*, em seu sentido mais comum, equivale à expressão *fumus comissi delicti* ou fumaça do cometimento de crime, largamente utilizada no Brasil. A expressão é também empregada com o sentido genérico de probabilidade, sem necessariamente se referir a probabilidade de cometimento de crime. Ver, no item 4.3, nosso entendimento sobre os conceitos de plausibilidade ou probabilidade a nortear o exame do cabimento de medidas cautelares.

[258] ESTADOS UNIDOS DA AMÉRICA. United States Court of Appeals for the Fourth Circuit. United States v. Appelbaum. 2013 U.S. App. LEXIS 1746; 41 Media L. Rep. 1177. Disponível em: <http://www.lexisnexis.com/hottopics/lnacademic/?.> Acesso em: 02 mar 2013: "To obtain records of stored electronic communications, such as a subscriber's name, address, length of subscription, and other like data, the government must secure either a warrant pursuant to Federal Rule of Criminal Procedure 41, or a court order under 18 U.S.C. § 2703(d). 18 U.S.C. § 2703(c). Orders issued under § 2703(d) may be granted if the government 'offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.' 18 U.S.C. § 2703(d). This is essentially a reasonable suspicion standard."

3.1.5. Interceptação das comunicações eletrônicas

A *Section* 2518 do *Title* 18 do *United States Code* (USC) dispõe que o pedido de autorização ou aprovação[259] da interceptação deverá ser escrito sob juramento ou sob o compromisso da verdade prestado perante um juiz competente[260], devendo conter, antes de tudo, a declaração do peticionante de sua autoridade para subscrever o requerimento. Isto porque um pedido de interceptação de comunicações ou de aprovação de interceptação só poderá ser subscrito por quem possua autorização do *prosecutor*[261] ou de alguém que o represente[262].

O pedido deverá conter a identidade do investigador e de quem autorizou a formulação do pedido e a descrição completa dos fatos e circunstâncias nas quais o investigador se baseou para justificar sua crença na necessidade de uma autorização para interceptação, incluindo detalhes sobre o delito que foi cometido, que esteja em execução no momento do pedido ou que esteja prestes a ser cometido. Deverá conter, também, uma descrição da natureza e do local em que estarão os aparelhos a serem interceptados ou a indicação do local em que estão ocorrendo as comunicações a serem interceptadas, além de uma descrição do tipo de comunicações cuja interceptação é solicitada e a identidade da pessoa, caso conhecida, que esteja cometendo o crime e cujas comunicações devam ser interceptadas. Precisará conter, ainda, uma declaração completa das medidas investigatórias que foram tentadas e tenham falhado ou a razão pela qual elas, razoavelmente, aparentam ser de sucesso improvável, se tentadas, ou perigosas demais. Deve indicar o período durante o qual se pretende manter a

---

[259] A existência do conceito de aprovação (*approval*) de uma interceptação se deve à possibilidade, na legislação dos Estados Unidos, de que a interceptação ocorra sem autorização judicial para que, posteriormente, seja objeto de aprovação por um juiz. As hipóteses em que tal medida é permitida constam no *Title* 18 USC § 2518 (7) e serão abordadas ainda no presente capítulo.

[260] 18 USC § 2518. "Procedure for interception of wire, oral, or electronic communications. **1)** Each application for an order authorizing or approving the interception of a wire, oral, or electronic communication under this chapter shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application." (Disponível em: <http://www.law.cornell.edu/uscode/text/18/2518>. Acesso em: 27 jan. 2013).

[261] O *prosecutor* é o representante do Estado responsável pela acusação. Mesmo ciente das diferenças fundamentais existentes entre os ordenamentos norte-americano e brasileiro, é possível afirmar que a figura do *prosecutor* corresponde ao Promotor de Justiça ou, na esfera federal, do Procurador da República.

[262] 18 USC § 2516. "Authorization for interception of wire, oral, or electronic communications. … (3) Any attorney for the Government (as such term is defined for the purposes of the Federal Rules of Criminal Procedure) may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant, in conformity with section 2518 of this title, an order authorizing or approving the interception of electronic communications by an investigative or law enforcement officer having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of any Federal felony." (Disponível em: <http://www.law.cornell.edu/uscode/text/18/2516>. Acesso em: 27 jan. 2013).

interceptação ou, caso se trate de comunicação do tipo que não permita a identificação do momento em que se deu o início da conversa, uma descrição dos fatos que demonstrem haver *probable cause* de que outras comunicações do mesmo tipo irão ocorrer posteriormente. Exige-se também uma declaração completa dos fatos relativos aos pedidos anteriores de interceptação ou aprovação de interceptação, dirigidos a qualquer juiz envolvendo qualquer das mesmas pessoas, aparelhos ou locais especificados no pedido, bem como a providência tomada pelo juiz em cada um daqueles casos pretéritos. Quando se tratar de pedido de prorrogação de interceptação já deferida, será necessário haver uma declaração expondo os resultados até então obtidos ou uma explanação razoável acerca da falha em obtê-los[263].

Extrai-se do trecho acima que a legislação norte-americana admite a interceptação de comunicações de modo preventivo, ou seja, para investigar ou impedir um crime futuro.

Observa-se, também, que a interceptação é tratada, ao menos na lei, como uma medida gravosa que só deve ser tentada em último caso, já que há uma exigência de que o requerente relate as medidas investigatórias que já foram tentadas previamente e que tenham falhado ou as razões para se acreditar que tais medidas não funcionariam ou que seriam perigosas demais.

É também digna de nota a imposição de que o requerente exponha detalhes relativos a interceptações requeridas anteriormente em relação àqueles mesmos investigados ou àqueles mesmos aparelhos e o que decidiu o juiz em cada caso, como forma de dar ao tribunal ao qual couber a decisão uma visão mais ampla do caso, reduzindo as possibilidades de indução dos juízes a erro.

---

[263] 18 USC § 2518. "Procedure for interception of wire, oral, or electronic communications … Each application shall include the following information: (a) the identity of the investigative or law enforcement officer making the application, and the officer authorizing the application; (b) a full and complete statement of the facts and circumstances relied upon by the applicant, to justify his belief that an order should be issued, including (i) details as to the particular offense that has been, is being, or is about to be committed, (ii) except as provided in subsection (11), a particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted, (iii) a particular description of the type of communications sought to be intercepted, (iv) the identity of the person, if known, committing the offense and whose communications are to be intercepted; (c) a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous; (d) a statement of the period of time for which the interception is required to be maintained. If the nature of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular description of facts establishing probable cause to believe that additional communications of the same type will occur thereafter; (e) a full and complete statement of the facts concerning all previous applications known to the individual authorizing and making the application, made to any judge for authorization to intercept, or for approval of interceptions of, wire, oral, or electronic communications involving any of the same persons, facilities or places specified in the application, and the action taken by the judge on each such application; and (f) where the application is for the extension of an order, a statement setting forth the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results." (Disponível em: <http://www.law.cornell.edu/uscode/text/18/2518>. Acesso em: 13 fev. 2013).

Apresentado o pedido, o juiz, que poderá solicitar elementos adicionais, como oitivas e documentos[264], poderá deferir o pedido de interceptação (ou aprovar a interceptação já implementada) dentro de sua área de competência territorial ou, em caso de dispositivo móvel de interceptação autorizado por uma corte federal competente, até mesmo fora de sua competência territorial, desde que dentro dos Estados Unidos.

Para tanto, o juiz, com base nos fatos que lhe foram submetidos, precisará se convencer de que: (1) há *probable cause* para acreditar que um indivíduo está cometendo, cometeu ou está em vias de cometer um dos crimes previstos no catálogo que autoriza a interceptação eletrônica; (2) há *probable cause* de que a interceptação requerida captará comunicações relativas àquele crime; (3) procedimentos investigatórios normais tenham sido tentados e falharam ou que tais procedimentos, por sua natureza, sejam incapazes de atingir o objetivo probatório pretendido ou que tais procedimentos sejam perigosos demais; (4) há *probable cause* para se acreditar que os aparelhos a serem interceptados estejam sendo ou venham a ser usados, com alguma relação com o crime investigado, pela pessoa-alvo da medida, ou que estejam locados ou cadastrados em nome desta[265].

Quanto ao catálogo, acima mencionado, deixa-se de abordar aqui a extensa lista de crimes passíveis de interceptação de *wire* e *oral communications*[266], já que, em relação às *electronic communications*, a lei se limita a dispor que a interceptação destas poderá ser empregada na investigação de qualquer crime federal[267].

---

[264] 18 USC § 2518. "Procedure for interception of wire, oral, or electronic communications … (2) The judge may require the applicant to furnish additional testimony or documentary evidence in support of the application" (Disponível em: <http://www.law.cornell.edu/uscode/text/18/2518>. Acesso em: 16 fev. 2013).

[265] 18 USC § 2518. "Procedure for interception of wire, oral, or electronic communications … (3) Upon such application the judge may enter an ex parte order, as requested or as modified, authorizing or approving interception of wire, oral, or electronic communications within the territorial jurisdiction of the court in which the judge is sitting (and outside that jurisdiction but within the United States in the case of a mobile interception device authorized by a Federal court within such jurisdiction), if the judge determines on the basis of the facts submitted by the applicant that— (a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense enumerated in section 2516 of this chapter; (b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception; (c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous; (d) except as provided in subsection (11), there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person." (Disponível em: <http://www.law.cornell.edu/uscode/text/18/2518>. Acesso em: 16 fev. 2013).

[266] Ver 18 USC § 2516. Authorization for interception of wire, oral, or electronic communications (1) (a) a (t) (Disponível em: <http://www.law.cornell.edu/uscode/text/18/2516>. Acesso em: 13 fev. 2013).

[267] 18 USC § 2516. "Authorization for interception of wire, oral, or electronic communications ... (3) Any attorney for the Government (as such term is defined for the purposes of the Federal Rules of Criminal Procedure) may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant, in conformity with section 2518 of this title, an order authorizing or approving the interception of electronic communications by an investigative or law enforcement officer having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has

A supra referida exigência, de que o juiz vislumbre probabilidade de que os aparelhos a serem interceptados pertençam às pessoas-alvo da medida ou que venham a ser por elas utilizados, é dispensada desde que preenchidas as seguintes condições: o pedido, aprovado pelo procurador geral ou por seus assistentes mais imediatos, deve emanar de um investigador federal ou oficial da lei; deve identificar a pessoa que se acredite estar cometendo o crime e cujas comunicações se desejam interceptar e o peticionante demonstrar *probable cause* de que os atos daquela pessoa poderiam frustrar a interceptação de um aparelho específico; o juiz deve entender que tal demonstração foi feita adequadamente; e a ordem autorizando ou aprovando a interceptação deve ser limitada a um tempo razoável para se presumir que a pessoa-alvo da medida esteja razoavelmente próxima dos instrumentos através dos quais as comunicações serão ou tenham sido transmitidas[268].

O trecho acima, que menciona atos do investigado capazes de frustrar a interceptação através de trocas constantes de aparelhos, trata de uma questão controversa conhecida como *roving wiretap*, que se poderia traduzir como *monitoramento itinerante*. É assim que chamam, nos Estados Unidos, a forma de interceptação das comunicações quando não vinculadas ao nome de uma pessoa investigada, mas aos equipamentos que esta use ou que se suspeite que venha a usar. O método visa a evitar a frustração da medida através da troca constante de computadores, contas de e-mail ou identidades utilizadas pelo investigado. A controvérsia reside no fato de que o monitoramento indiscriminado de equipamentos, sem uma identificação prévia de *probable cause* em relação a uma determinada pessoa, feriria a exigência de individualização da Quarta Emenda. Foi diante de tal controvérsia que o *Patriot Act* de 2001[269] veio a ratificar tal possibilidade de monitoramento.

---

provided evidence of any Federal felony." (Disponível em: <http://www.law.cornell.edu/uscode/text/18/2516>. Acesso em: 13 fev. 2013).

[268] 18 USC § 2518. "Procedure for interception of wire, oral, or electronic communications … 11) The requirements of subsections (1)(b)(ii) and (3)(d) of this section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply if … (b) in the case of an application with respect to a wire or electronic communication — (i) the application is by a Federal investigative or law enforcement officer and is approved by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an acting Assistant Attorney General; (ii) the application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing that there is probable cause to believe that the person's actions could have the effect of thwarting interception from a specified facility; (iii) the judge finds that such showing has been adequately made; and (iv) the order authorizing or approving the interception is limited to interception only for such time as it is reasonable to presume that the person identified in the application is or was reasonably proximate to the instrument through which such communication will be or was transmitted." (Disponível em: <http://www.law.cornell.edu/uscode/text/18/2518>. Acesso em: 13 fev. 2013).

[269] ESTADOS UNIDOS DA AMÉRICA. U.S. Government Printing Office. Public Law 107-56-Oct. 26, 2001, Uniting and strengthening america by providing appropriate tools required to intercept and obstruct terrorism (USA Patriot Act) act of 2001. Disponivel em: <http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf>. Acesso em: 16 fev. 2013: "Section 206. Roving Surveillance Authority Under the Foreign Intelligence Surveillance Act Of 1978. Section 105(c)(2)(B) of the Foreign Intelligence Surveillance Act of 1978

A decisão que autorizar ou aprovar a interceptação deverá especificar: (1) a identidade da pessoa a ser interceptada, se conhecida; (2) a natureza e localização dos aparelhos a serem interceptados; (3) o tipo de comunicação a ser interceptada e o crime ao qual ela se liga; (4) o órgão autorizado a promover a interceptação e a pessoa que autorizou a formulação do pedido; e (5) o período dentro do qual a interceptação está sendo autorizada, incluindo uma declaração quanto a dever ou não a interceptação cessar automaticamente tão logo a comunicação pretendida seja captada[270].

A norma acima mostra que a decisão que autoriza a interceptação poderá, além de simplesmente fixar a duração da medida (cujo prazo máximo é de 30 dias, 18 USC § 2518(5)), determinar que esta cesse tão logo seja captada a comunicação pretendida.

Nenhuma decisão judicial pode autorizar ou aprovar a interceptação por um período maior do que o necessário para atingir o objetivo da autorização. Tal período nunca será maior do que trinta dias, prazo que começa a ser contado na manhã do dia em que a interceptação começa a ser executada ou, senão, dez dias depois que a ordem for expedida. Prorrogações poderão ser deferidas, porém não por período superior àquele que o juiz julgar necessário para efetivar o propósito da prorrogação, que nunca excederá trinta dias. Todas as autorizações para interceptação ou suas prorrogações devem conter determinação de que sejam cumpridas o mais rápido possível, bem como para que se minimize o acesso a comunicações não contempladas pela autorização e de que a medida deve cessar tão logo se atinja o objetivo para o qual foi autorizada ou, em qualquer hipótese, de que deve cessar no prazo máximo de trinta dias. Caso as comunicações interceptadas estejam em algum código ou língua estrangeira, não havendo um especialista naquele código ou na língua estrangeira disponível durante o curso da interceptação, a decifração pode ser realizada tão logo seja possível, após a interceptação. A interceptação pode ser conduzida integralmente ou em parte

---

(50 U.S.C. 1805(c)(2)(B)) is amended by inserting, 'or in circumstances where the Court finds that the actions of the target of the application may have the effect of thwarting the identification of a specified person, such other persons,' after 'specified person'."

[270] 18 USC § 2518. "Procedure for interception of wire, oral, or electronic communications … (4) Each order authorizing or approving the interception of any wire, oral, or electronic communication under this chapter shall specify: (a) the identity of the person, if known, whose communications are to be intercepted; (b) the nature and location of the communications facilities as to which, or the place where, authority to intercept is granted; (c) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates; (d) the identity of the agency authorized to intercept the communications, and of the person authorizing the application; and **(e)** the period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained." (Disponível em: <http://www.law.cornell.edu/uscode/text/18/2518>. Acesso em: 02 fev. 2013).

por agentes do governo ou por pessoa que atue sob contratação do governo, impondo-se, neste caso, a supervisão de um investigador ou oficial autorizado a conduzir a interceptação[271].

Interessante a previsão de data específica a ser considerada como o início da interceptação, de modo a permitir um controle rígido da obediência aos prazos, evitando-se a captação e utilização probatória de comunicação captada ilicitamente.

Uma determinação judicial autorizando interceptação de comunicação obriga que o provedor de comunicações, proprietário, zelador ou outro funcionário forneça ao requerente, de imediato, todas as informações, equipamentos e assistência técnica necessários a efetivar a interceptação de forma discreta e com o mínimo de interferência nos serviços que o provedor, proprietário, zelador ou outro funcionário esteja prestando à pessoa-alvo da interceptação. Qualquer provedor que houver fornecido equipamento ou assistência técnica deve ser compensado por despesas razoavelmente geradas por tal fornecimento. O juiz poderá proferir uma determinação específica para compelir o provedor a fornecer assistência técnica sob a autoridade do chamado *Communications Assistance for Law Enforcement Act*[272], uma alteração promovida no *United States Code* (USC) (*Title* 47, *Sections* 1001 a 1010) em 1994,

---

[271] 18 USC § 2518. "Procedure for interception of wire, oral, or electronic communications … (5) No order entered under this section may authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days. Such thirty-day period begins on the earlier of the day on which the investigative or law enforcement officer first begins to conduct an interception under the order or ten days after the order is entered. Extensions of an order may be granted, but only upon application for an extension made in accordance with subsection (1) of this section and the court making the findings required by subsection (3) of this section. The period of extension shall be no longer than the authorizing judge deems necessary to achieve the purposes for which it was granted and in no event for longer than thirty days. Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days. In the event the intercepted communication is in a code or foreign language, and an expert in that foreign language or code is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. An interception under this chapter may be conducted in whole or in part by Government personnel, or by an individual operating under a contract with the Government, acting under the supervision of an investigative or law enforcement officer authorized to conduct the interception" (Disponível em: <http://www.law.cornell.edu/uscode/text/18/2518>. Acesso em: 03 fev. 2013).

[272] 18 USC § 2518. "Procedure for interception of wire, oral, or electronic communications … (4) … An order authorizing the interception of a wire, oral, or electronic communication under this chapter shall, upon request of the applicant, direct that a provider of wire or electronic communication service, landlord, custodian or other person shall furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider, landlord, custodian, or person is according the person whose communications are to be intercepted. Any provider of wire or electronic communication service, landlord, custodian or other person furnishing such facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing such facilities or assistance. Pursuant to section 2522 of this chapter, an order may also be issued to enforce the assistance capability and capacity requirements under the Communications Assistance for Law Enforcement Act." (Disponível em: <http://www.law.cornell.edu/uscode/text/18/2518>. Acesso em: 02 fev. 2013).

que instituiu uma série de obrigações e penalidades para provedores de serviços de comunicação que não colaborassem com a viabilização das medidas de interceptação.

O juiz pode exigir relatórios em intervalos de tempo por ele fixados, dispondo sobre o andamento da interceptação, o alcance ou não do objetivo autorizado e a necessidade para a continuidade da medida[273].

O dispositivo acima demonstra que a interceptação de comunicações foi concebida pelo Congresso norte-americano como uma medida que pode ser requerida e deferida visando à captação precisa de um diálogo específico.

O conteúdo de qualquer interceptação deverá, se possível, ser gravado em fita ou dispositivo comparável, de uma forma que a gravação fique protegida contra edição ou outras alterações. Imediatamente após o término da interceptação ou prorrogações, as gravações devem ser disponibilizadas ao juiz que fizer tal exigência. O local de custódia das gravações será definido pelo juiz. As gravações não devem ser destruídas a menos que haja determinação do juiz, devendo, em qualquer hipótese, ser preservadas por dez anos[274].

Cópias das gravações poderão ser extraídas desde que para o adequado desempenho das obrigações funcionais do oficial que as usará ou do oficial que enviou ou recebeu o material. A presença do selo do juiz que deferiu a ordem ou de explicação satisfatória para sua ausência será pré-requisito para a utilização probatória do material interceptado ou de elemento dele derivado. Referido selo deverá ser posto nos pedidos e nas ordens. A custódia das ordens e pedidos será feita em local definido pelo juiz. Tais ordens e pedidos somente deverão ser divulgados mediante demonstração de uma boa causa perante o juiz e não deverão ser destruídos senão por ordem deste, devendo, em qualquer hipótese, ser preservados por dez anos. Qualquer violação dessas normas poderá ser punida como desídia por parte do juiz que deferiu ou indeferiu a medida. Dentro de um prazo razoável, de até noventa dias após a formulação de um pedido de aprovação de interceptação que tenha sido negado ou após o

---

[273] 18 USC § 2518. "Procedure for interception of wire, oral, or electronic communications … (6) Whenever an order authorizing interception is entered pursuant to this chapter, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require." (Disponível em: <http://www.law.cornell.edu/uscode/text/18/2518>. Acesso em: 03 fev. 2013).

[274] 18 USC § 2518. "Procedure for interception of wire, oral, or electronic communications … (8) (a) The contents of any wire, oral, or electronic communication intercepted by any means authorized by this chapter shall, if possible, be recorded on tape or wire or other comparable device. The recording of the contents of any wire, oral, or electronic communication under this subsection shall be done in such a way as will protect the recording from editing or other alterations. Immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under his directions. Custody of the recordings shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing or denying judge and in any event shall be kept for ten years." (Disponível em: <http://www.law.cornell.edu/uscode/text/18/2518>. Acesso em: 09 fev. 2013).

término do período autorizado para uma interceptação, o juiz deverá receber um relatório relatando os fatos que foram objeto da ordem ou do pedido de interceptação, a data da expedição da ordem e o período da interceptação autorizada, aprovada ou reprovada ou o indeferimento do pedido e os fatos sobre os quais se conseguiu ou não amealhar elementos. Quando necessário, o prazo para elaboração de tal relatório poderá ser prorrogado pelo juiz. O juiz, mediante uma petição, poderá, conforme sua discricionariedade, disponibilizar à pessoa interceptada ou a seu advogado, para inspeção, os trechos das comunicações interceptadas, pedidos e decisões, que ele juiz determinar que sejam do interesse da justiça[275].

O conteúdo de qualquer interceptação ou prova dele derivada somente poderá ser utilizado ou divulgado em algum julgamento, audiência ou outro procedimento se a cópia da decisão que autorizou ou aprovou a interceptação e da petição que a requereu for disponibilizada às partes no mínimo dez dias antes, podendo tal prazo ser reduzido quando o juiz entender que não é possível fazer tal disponibilização com tanta antecedência, desde que deste atraso não decorrerá prejuízo para as partes[276].

Nota-se que inexiste o direito defensivo de ter ciência completa de como se desenvolveu o processo investigatório e se houve obediência às prescrições legais. O que há é

---

[275] 18 USC § 2518. "Procedure for interception of wire, oral, or electronic communications … (8) (a) … Duplicate recordings may be made for use or disclosure pursuant to the provisions of subsections (1) and (2) of section 2517 of this chapter for investigations. The presence of the seal provided for by this subsection, or a satisfactory explanation for the absence thereof, shall be a prerequisite for the use or disclosure of the contents of any wire, oral, or electronic communication or evidence derived therefrom under subsection (3) of section 2517. (b) Applications made and orders granted under this chapter shall be sealed by the judge. Custody of the applications and orders shall be wherever the judge directs. Such applications and orders shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction and shall not be destroyed except on order of the issuing or denying judge, and in any event shall be kept for ten years. (c) Any violation of the provisions of this subsection may be punished as contempt of the issuing or denying judge. (d) Within a reasonable time but not later than ninety days after the filing of an application for an order of approval under section 2518 (7)(b) which is denied or the termination of the period of an order or extensions thereof, the issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, an inventory which shall include notice of— (1) the fact of the entry of the order or the application; (2) the date of the entry and the period of authorized, approved or disapproved interception, or the denial of the application; and (3) the fact that during the period wire, oral, or electronic communications were or were not intercepted. The judge, upon the filing of a motion, may in his discretion make available to such person or his counsel for inspection such portions of the intercepted communications, applications and orders as the judge determines to be in the interest of justice. On an ex parte showing of good cause to a judge of competent jurisdiction the serving of the inventory required by this subsection may be postponed." (Disponível em: <http://www.law.cornell.edu/uscode/text/18/2518>. Acesso em: 09 fev. 2013).

[276] 18 USC § 2518. "Procedure for interception of wire, oral, or electronic communications … (9) The contents of any wire, oral, or electronic communication intercepted pursuant to this chapter or evidence derived therefrom shall not be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in a Federal or State court unless each party, not less than ten days before the trial, hearing, or proceeding, has been furnished with a copy of the court order, and accompanying application, under which the interception was authorized or approved. This ten-day period may be waived by the judge if he finds that it was not possible to furnish the party with the above information ten days before the trial, hearing, or proceeding and that the party will not be prejudiced by the delay in receiving such information." (Disponível em: <http://www.law.cornell.edu/uscode/text/18/2518>. Acesso em: 03 fev. 2013).

um direito limitadíssimo de que o réu tenha acesso àqueles pedidos e decisões autorizativas de interceptação que deram origem a trechos que serão, efetivamente, utilizados como prova. Não é automática a obrigatoriedade de se submeter o material captado ao juiz, o que só ocorrerá se este assim o exigir, bem como não é automático o direito do investigado de, após a conclusão da interceptação, ter acesso ao que foi captado e à documentação relativa a requerimentos e decisões judiciais.

A *Section* 2511(1) do *Title* 18 estabelece que aquele que, sem autorização legal, interceptar comunicações, usar produto de interceptação ou divulgá-lo deverá ser punido com pena privativa de liberdade de até cinco anos e/ou multa de até US$ 250,000 ou, se da conduta resultar ganho pecuniário para o agente ou prejuízo para o lesado, até o dobro do valor desse ganho ou prejuízo[277].

3.1.6. Interceptação com dispensa de autorização judicial

Qualquer oficial investigador, designado especialmente pelo procurador-geral ou por seus representantes mais imediatos, que se convença de que haja uma situação de emergência que não possa esperar uma autorização para interceptação e de que essa emergência envolva perigo imediato de vida ou de graves danos físicos à pessoa, ou atividades conspiratórias próprias de crime organizado ou que ameacem a segurança nacional poderá promover interceptação desde que, dentro de 48 horas, apresente um pedido de aprovação.

Se, no entanto, uma aprovação judicial não for obtida, a interceptação deverá cessar assim que for captada a comunicação desejada ou assim que o pedido de aprovação for

[277] 18 USC § 2511. "Interception and disclosure of wire, oral, or electronic communications prohibited (1) Except as otherwise specifically provided in this chapter any person who— (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication; (b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication … shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5). … (4) (a) Except as provided in paragraph (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both." (Disponível em: <http://www.law.cornell.edu/uscode/text/18/2511>. Acesso em: 11 fev. 2013) e 18 USC § 3571. "Sentence of fine … b) Fines for Individuals.— Except as provided in subsection (e) of this section, an individual who has been found guilty of an offense may be fined not more than the greatest of— … (3) for a felony, not more than $250,000; … (d) Alternative Fine Based on Gain or Loss.— If any person derives pecuniary gain from the offense, or if the offense results in pecuniary loss to a person other than the defendant, the defendant may be fined not more than the greater of twice the gross gain or twice the gross loss, unless imposition of a fine under this subsection would unduly complicate or prolong the sentencing process." (Disponível em: <http://www.law.cornell.edu/uscode/text/18/3571>. Acesso em: 11 fev. 2013).

indeferido, dependendo de qual dos eventos ocorra primeiro. Caso a aprovação seja indeferida ou caso a medida de interceptação chegue naturalmente a seu término sem que uma aprovação tenha sido expedida, qualquer material captado deverá ser considerado ilícito, circunstância em que o solicitante da ordem deverá elaborar um relatório a ser fornecido ao juiz[278].

Digna de nota a previsão legal de dispensa de autorização judicial quando diante de atividades conspiratórias, ato que, no Brasil, seria atípico. Trata-se, ao que parece, de uma espécie de aposta do órgão de investigação na futura e incerta aprovação da interceptação que ele entendeu por promover, sob o risco de se considerar ilícito todo o material que vier a captar.

Para além das já retratadas hipóteses de interceptação a ser submetida a uma aprovação judicial dentro de quarenta e oito horas[279], há previsão legal trazida pelo *Foreign Intelligence Surveillance Act* (FISA) de que o Presidente da República, através do procurador geral, poderá autorizar monitoramento eletrônico sem ordem judicial para obter informações sobre inteligência estrangeira por períodos de até um ano, desde que o procurador-geral declare, sob juramento: (a) que o monitoramento é exclusivamente voltado para a obtenção de comunicações entre poderes estrangeiros, de modo a captar dados de inteligência técnica a eles pertencentes ou, ainda, comunicação advinda de um local submetido ao controle de um poder estrangeiro; (b) que não há risco de que a vigilância venha a captar o conteúdo de qualquer comunicação em que uma pessoa dos Estados Unidos seja interlocutora; e (c) que,

---

[278] 18 USC § 2518. "Procedure for interception of wire, oral, or electronic communications … (7) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that— (a) an emergency situation exists that involves— (i) immediate danger of death or serious physical injury to any person, (ii) conspiratorial activities threatening the national security interest, or (iii) conspiratorial activities characteristic of organized crime, that requires a wire, oral, or electronic communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and (b) there are grounds upon which an order could be entered under this chapter to authorize such interception, may intercept such wire, oral, or electronic communication if an application for an order approving the interception is made in accordance with this section within forty-eight hours after the interception has occurred, or begins to occur. In the absence of an order, such interception shall immediately terminate when the communication sought is obtained or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied, or in any other case where the interception is terminated without an order having been issued, the contents of any wire, oral, or electronic communication intercepted shall be treated as having been obtained in violation of this chapter, and an inventory shall be served as provided for in subsection (d) of this section on the person named in the application." (Disponível em: <http://www.law.cornell.edu/uscode/text/18/2518>. Acesso em: 03 fev. 2013).

[279] Como visto acima, no 18 USC § 2518(7)(a), a possibilidade de interceptação condicionada a aprovação judicial posterior é restrita aos casos de perigo imediato de vida ou de graves danos físicos à pessoa, atividades conspiratórias que ameacem a segurança nacional e atividades conspiratórias características de crime organizado.

em caso de captação de comunicações de pessoas dos Estados Unidos, estas serão mantidas em caráter reservado, exceto se as próprias consentirem no contrário[280].

3.1.7 Exclusão da prova ilícita

A *Section* 2515 do *Title* 18 do USC leva o nome de "proibição do uso probatório de interceptação de *wire* ou *oral communications*" e dispõe que, sempre que qualquer *wire* ou *oral communication* for interceptada, nenhuma parte do conteúdo de tal comunicação e nenhuma prova dela derivada poderá ser recebida como prova em qualquer julgamento, audiência ou outro procedimento ou perante qualquer corte, grande júri, departamento, oficial, agência, corpo regulatório, comitê legislativo ou outra autoridade dos Estados Unidos, do estado ou de sua subdivisão política, se a divulgação do material for violadora "deste capítulo" (no caso, trata-se do *Title* 18, *Part* I, *Chapter* 119)[281].

Ver-se-á adiante, no entanto, que não há dispositivo análogo que seja aplicável às *electronic communications*.

A *Section* 2518 prevê o remédio a ser adotado no sentido de suprimir material decorrente de interceptação ilegal, dispondo que qualquer pessoa prejudicada em algum

---

[280] 50 USC § 1802 – "Electronic surveillance authorization without court order; certification by Attorney General; reports to Congressional committees; transmittal under seal; duties and compensation of communication common carrier; applications; jurisdiction. a) (1) Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this subchapter to acquire foreign intelligence information for periods of up to one year if the Attorney General certifies in writing under oath that— (A) the electronic surveillance is solely directed at— (i) the acquisition of the contents of communications transmitted by means of communications used exclusively between or among foreign powers, as defined in section 1801 (a)(1), (2), or (3) of this title; or (ii) the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive control of a foreign power, as defined in section 1801 (a)(1), (2), or (3) of this title; (B) there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party; and (C) the proposed minimization procedures with respect to such surveillance meet the definition of minimization procedures under section 1801 (h) of this title; and if the Attorney General reports such minimization procedures and any changes thereto to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence at least thirty days prior to their effective date, unless the Attorney General determines immediate action is required and notifies the committees immediately of such minimization procedures and the reason for their becoming effective immediately" (Disponível em: <http://www.law.cornell.edu/uscode/text/50/1802>. Acesso em: 02 mar. 2013).

[281] 18 USC § 2515. "Prohibition of use as evidence of intercepted wire or oral communications – Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing, or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee, or other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter" (Disponível em: <http://www.law.cornell.edu/uscode/text/18/2515>. Acesso em: 12 fev. 2013).

julgamento, audiência ou procedimento, perante qualquer corte, departamento, oficial, agência, corpo regulatório ou outra autoridade dos Estados Unidos, estado ou subdivisão política pode atuar no sentido de suprimir o conteúdo de alguma interceptação ou prova derivada quando: a comunicação houver sido interceptada ilegalmente; a decisão que tiver autorizado ou aprovado a interceptação for insuficiente; ou quando a interceptação não houver sido promovida em conformidade com a autorização ou aprovação.

A petição para se obter a ordem de supressão amparada na *Section* 2518 deve ser feita antes do julgamento, audiência ou procedimento, a menos que não haja oportunidade para fazê-lo ou o requerente não conheça ainda os motivos do pedido. Se o pedido for deferido, o conteúdo da interceptação e as provas dele derivadas serão consideradas ilícitas. O juiz, diante de tal pedido, poderá, dentro de sua discricionariedade, disponibilizar à pessoa prejudicada ou ao seu advogado, para inspeção, partes da interceptação ou prova dela derivada que ele juiz determine ser do interesse da justiça. Além de outras hipóteses em que caiba apelação, assegura-se ao órgão de acusação o direito de apelar de uma decisão deferindo a supressão de material interceptado ou indeferindo uma aprovação de interceptação, devendo ele, nesse caso, declarar que o apelo não tem finalidade procrastinatória. O prazo para tal apelação, que deve ser processada diligentemente, é de trinta dias a contar do dia em que a decisão for proferida[282].

Observa-se que, até mesmo diante de pedido de supressão de comunicação, cuja interceptação se reputou ilícita, o acesso ao material captado e às provas dele derivadas é

---

[282] 18 USC § 2518. "Procedure for interception of wire, oral, or electronic communications … (10) (a) Any aggrieved person in any trial, hearing, or proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the contents of any wire or oral communication intercepted pursuant to this chapter, or evidence derived therefrom, on the grounds that— (i) the communication was unlawfully intercepted; (ii) the order of authorization or approval under which it was intercepted is insufficient on its face; or (iii) the interception was not made in conformity with the order of authorization or approval. Such motion shall be made before the trial, hearing, or proceeding unless there was no opportunity to make such motion or the person was not aware of the grounds of the motion. If the motion is granted, the contents of the intercepted wire or oral communication, or evidence derived therefrom, shall be treated as having been obtained in violation of this chapter. The judge, upon the filing of such motion by the aggrieved person, may in his discretion make available to the aggrieved person or his counsel for inspection such portions of the intercepted communication or evidence derived therefrom as the judge determines to be in the interests of justice. (b) In addition to any other right to appeal, the United States shall have the right to appeal from an order granting a motion to suppress made under paragraph (a) of this subsection, or the denial of an application for an order of approval, if the United States attorney shall certify to the judge or other official granting such motion or denying such application that the appeal is not taken for purposes of delay. Such appeal shall be taken within thirty days after the date the order was entered and shall be diligently prosecuted. (c) The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications" (Disponível em: <http://www.law.cornell.edu/uscode/text/18/2518>. Acesso em: 03 fev. 2013).

restrito e fica submetido a uma discricionariedade do magistrado, como se ele se substituísse à defesa na avaliação de quais elementos lhe são interessantes e quais não o são.

No caso *United States v. Appelbaum*, a *United States Court of Appeals for the Fourth Circuit* manteve a decisão recorrida de impedir o acesso do defensor às ordens judiciais que requisitaram conteúdo de comunicações eletrônicas armazenadas, mesmo já estando inaugurada a fase de julgamento. Sustenta o acórdão que (1) não se trata de um direito de acesso que tem sido historicamente garantido à imprensa e ao público em geral; e (2) o acesso público, nesse caso, não desempenha um papel importante no funcionamento do caso sob julgamento. Destacou, ainda, que a fase em que o conteúdo de comunicações armazenadas é requisitado, que chamou de "*investigative, pre-grand jury, pre-indictment phase*" é, por sua própria natureza, sigilosa, devendo-se ocultar do investigado os movimentos investigatórios, sob pena de frustração da medida. Argumentou o recorrente, no entanto, que não haveria legitimidade para uma restrição contínua do acesso, mas tão somente até a conclusão da medida, ao que refutou a Corte sustentando que o sigilo contínuo se prestaria a prevenir potenciais pessoas a serem investigadas de serem avisadas, ou de alterarem seus comportamentos para frustrar investigações e que o fato de ser o caso de grande repercussão não justificaria a divulgação do material, devendo-se manter o sigilo tal qual nos casos das investigações dos atentados de Oklahoma e das Torres Gêmeas[283].

---

[283] ESTADOS UNIDOS DA AMÉRICA. United States Court of Appeals for the Fourth Circuit. United States v. Appelbaum. 2013 U.S. App. LEXIS 1746; 41 Media L. Rep. 1177. Disponível em: <http://www.lexisnexis.com/hottopics/lnacademic/?.> Acesso em: 02 mar 2013: "We first address the basis for our jurisdiction over this matter. We have stated '[m]andamus, not appeal,' is the preferred method of review for orders restricting [access] to criminal proceedings.' ' Balt. Sun Co. v. Goetz, 886 F.2d 60, 63 (4th Cir. 1989) (quoting Wash. Post Co. v. Soussoudis, 807 F.2d 383, 388 (4th Cir. 1986)). As mandamus is the preferred method for reviewing courts' orders restricting access to criminal proceedings, we treat Subscribers' appeal as a petition for mandamus, and we have jurisdiction under the All Writs Act, 28 U.S.C. § 1651. See Wash. Post Co., 807 F.2d at 388.3 ... Subscribers next contend that the district court erred in permitting the Other § 2703(d) Orders and related documents to remain sealed because these documents are subject to the right of access. … To determine whether the First Amendment provides a right to access § 2703(d) orders and proceedings, we employ the 'experience and logic' test, asking: '(1) 'whether the place and process have historically been open to the press and general public,' and (2) 'whether public access plays a significant positive role in the functioning of the particular process in question.' Goetz, 886 F.2d at 64 (quoting Press-Enterprise Co. v. Superior Court, 478 U.S. 1, 8-10, 106 S. Ct. 2735, 92 L. Ed. 2d 1 (1988)). Here, neither prong is satisfied. Subscribers concede that there is no long tradition of access specifically for § 2703(d) orders, given that the SCA was enacted in 1986. However, they argue that under *Press-Enterprise*, where a relatively new process is at issue, courts focus on the logic prong. Our post-*Press Enterprise* precedent makes clear that both the experience and logic prongs are required. *See Goetz*, 886 F.2d at 64 (stating a conjunctive test); *see also United States v. Gonzales*, 150 F.3d 1246, 1258 (10th Cir. 1998) (citing *Goetz* for the proposition that some courts adopt the approach that *Press-Enterprise* requires satisfaction of *both* prongs). … The § 2703(d) process is investigative, and openness of the orders does not play a significant role in the functioning of investigations. Section 2703(d) proceedings consist of the issuance of and compliance with § 2703(d) orders, are *ex parte* in nature, and occur at the investigative, pre-grand jury, pre-indictment phase of what may or may not mature into an indictment. Pre-indictment investigative processes 'where privacy and secrecy are the norm' 'are not amenable to the practices and procedures employed in connection with other judicial proceedings.' *See In re Sealed Case*, 199 F.3d 522, 526, 339 U.S. App. D.C. 309 (D.C. Cir. 2000). … Subscribers contend that the Government lacks a legitimate interest

O dispositivo legal citado no início deste item, no entanto, que prevê o remédio através do qual se pleiteia a supressão de comunicações ilícitas (18 USC § 2518(1)(a)), não contempla as *electronic communications*, mas somente as *wire* e *oral communications*, o que se deve ao momento em que a lei foi aprovada pelo Congresso, 1986, anterior à internet e à *World Wide Web*.

No entanto, no caso *United States v. Steiger*, o acusado invocou, a *contrario sensu*, a *Section* 2517, que dispõe que as *electronic communications* poderão ser utilizadas se seguidas as prescrições legais[284], tendo a *United States Court of Appeals for the Eleventh Circuit* entendido que a lei não apresenta base para se determinar a supressão de comunicações eletrônicas, mas apenas sanções criminais e cíveis[285]. A Corte não chegou a se pronunciar se a supressão pleiteada poderia advir da *Section* 2517, tal qual invocado, pois entendeu que a

---

in continued sealing, and the magistrate judge 'improperly relegated,' and failed to weigh the public's 'strong' interest in having access to the § 2703 orders and motions. Among the identified public interests, Subscribers state an interest in: participating in a matter of national importance, which is the ongoing debate about WikiLeaks' publications; understanding the nature and scope of the government's electronic surveillance of internet activities; and to the extent the § 2703 orders have not been complied with, providing Subscribers with an opportunity to challenge the orders to preclude a violation of their constitutional rights. Subscribers' contentions fail for several reasons. First, the record shows that the magistrate judge considered the stated public interests [*23] and found that the Government's interests in maintaining the secrecy of its investigation, preventing potential subjects from being tipped off, or altering behavior to thwart the Government's ongoing investigation, outweighed those interests. Further, we agree with the magistrate judge's findings that the common law presumption of access to § 2703 orders is outweighed by the Government's interest in continued sealing because the publicity surrounding the WikiLeaks investigation does not justify its unsealing. The mere fact that a case is high profile in nature does not necessarily justify public access. *See United States v. McVeigh*, 119 F.3d 806 (10th Cir. 1997) (upholding the sealing of documents in the Oklahoma City bombing trial); *Moussaoui*, 65 F. App'x at 887 n.5 (upholding sealed classified documents related to the terrorist attacks on September 11, 2001). Additionally, Subscribers' contention that the balance of interests tips in the public's favor because the Government approved the disclosure of the existence of its investigation by moving the district court to unseal the Twitter Order is adequately counterbalanced by the magistrate judge's finding that the 'sealed documents at issue set forth sensitive nonpublic facts, including the identity of targets and witnesses in an ongoing criminal investigation.' The magistrate judge also found that 'there are legitimate concerns that publication of the documents at this juncture will hamper the investigatory process.' Regardless of the execution of, or compliance with, the Other § 2703(d) Orders, to allow the public or Subscribers access to the orders after such a finding is an improper means of circumventing the SCA's clear assessment that in some instances, non-disclosure of the existence of the orders is warranted. *Accord* 18 U.S.C. § 2705(b). As such, the magistrate judge did not abuse her discretion in finding that the Government's interests are significantly countervailing, and outweigh the public's common law presumption of access. Hence, the substantive requirements to sealing are met."

[284] 18 USC § 2517. "Authorization for disclosure and use of intercepted wire, oral, or electronic communications … (3) Any person who has received, by any means authorized by this chapter, any information concerning a wire, oral, or electronic communication, or evidence derived therefrom intercepted in accordance with the provisions of this chapter may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any State or political subdivision thereof." (Disponível em: http://www.law.cornell.edu/uscode/text/18/2517. Acesso em 12.02.2013).

[285] ESTADOS UNIDOS DA AMÉRICA. United States Court of Appeals for the Eleventh Circuit. United States v. Steiger. 318 F.3d 1039, 1050-52 (11th Cir. 2003). Disponível em: <http://www.lexisnexis.com/hottopics/lnacademic/?>. Acesso em: 12 fev. 2013: "We hold that the anonymous source did not intercept electronic communications in violation of the Wiretap Act. We also hold that while the Wiretap Act clearly provides criminal and civil sanctions for the unlawful interception of electronic communications, see 18 U.S.C. §§ 2511(1), (4), (5), 2520, the Act provides no basis for moving to suppress such communications."

aquisição do material eletrônico, no caso dois e-mails extraídos remotamente do disco rígido do computador do investigado, através do uso de um vírus, não se enquadrava em interceptação, pois não fora contemporânea, ou seja, a aquisição não se deu no momento da transmissão, tratando-se, portanto, de um resquício de uma comunicação pretérita[286].

O precedente registrou, ainda, além da ausência de remédio previsto em lei para se obter a supressão de comunicações eletrônicas armazenadas, o nível de proteção menor assegurado às *stored communications*, já que são menores as exigências legais para o acesso a estas[287].

Já no caso *United States v. Jones*, em que o acusado também invocou a *Section* 2517 para pleitear a supressão de comunicações eletrônicas, a *United States District Court for the District of Utah* afirmou, expressamente, que a falta de previsão das *electronic*

---

[286] ESTADOS UNIDOS DA AMÉRICA. United States Court of Appeals for the Eleventh Circuit. United States v. Steiger. 318 F.3d 1039, 1050-52 (11th Cir. 2003). Disponível em: <http://www.lexisnexis.com/hottopics/lnacademic/?>. Acesso em: 12 fev. 2013: "'Electronic communications' are defined in the Wiretap Act as 'any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce.' 18 U.S.C. § 2510(12). At least one Circuit has held that information stored on a server and conveyed from a private website to users clearly falls within the definition of 'electronic communications.' Konop, 302 F.3d at 876. Here, the source penetrated Steiger's computer by using a "Trojan Horse" virus that enabled him to discover and download files stored on Steiger's hard drive. That information was transferred from Steiger's computer to the source over one of the specified media and thus falls within the Wiretap Act's definition of 'electronic communications.' 'Interception' is defined as 'the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.' 18 U.S.C. § 2510(4). The Circuits which have interpreted this definition as applied to electronic communications have held that it encompasses only acquisitions contemporaneous with transmission. See Konop, 302 F.3d at 878-89 (withdrawing previous panel opinion at 236 F.3d 1035 (9th Cir. 2001) holding to the contrary); Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457 (5th Cir. 1994); see also United States v. Smith, 155 F.3d 1051 (9th Cir. 1998)."

[287] ESTADOS UNIDOS DA AMÉRICA. United States Court of Appeals for the Eleventh Circuit. United States v. Steiger. 318 F.3d 1039, 1050-52 (11th Cir. 2003). Disponível em: <http://www.lexisnexis.com/hottopics/lnacademic/?>. Acesso em: 12 fev. 2013: "The Ninth and Fifth Circuits also concluded that their reading of the Wiretap Act 'is consistent with the structure of the ECPA, which created the SCA for the express purpose of addressing 'access to stored . . . electronic communications and transactional records.' ' Konop, 302 F.3d at 878-79 (emphasis in original) (quoting S.Rep. No. 99-541 at 3); Steve Jackson Games, 36 F.3d at 463. These two cases reasoned that 'the level of protection provided stored communications under the SCA is considerably less than that provided by communications covered by the Wiretap Act. . . . [If] acquisition of a stored communication were an interception under the Wiretap Act, the government would have to comply with the more burdensome, more restrictive procedures of the Wiretap Act to do exactly what Congress apparently authorized it to do under the less burdensome procedures of the SCA. Congress could not have intended this result.' Konop, 302 F.3d at 879; see also Steve Jackson Games, 36 F.3d at 463. Though we agree with the Fifth and Ninth Circuits' interpretation of the Wiretap Act, we do not rely on this particular reasoning in doing so. See generally Konop, 302 F.3d at 889 (Reinhardt, J., dissenting in part) (explaining that 'the majority's interpretation of the Wiretap Act depends in part on a tortured reading of the Stored Communications Act'). The SCA creates criminal and civil penalties, but no exclusionary remedy, for unauthorized access to a 'facility through which an electronic communication service is provided' to 'obtain, alter, or prevent authorized access to a wire or electronic communication while it is in electronic storage in such system.' 18 U.S.C. § 2701 (emphasis added); see also 18 U.S.C. §§ 2707, 2708."

communications dentre aquelas dispostas na *Section* 2515 impediria que se determinasse a supressão de um conteúdo interceptado[288].

No caso *Jody Lee Miles v. State of Maryland*, uma apelação obrigatória contra sentença a pena de morte, a *Court of Appeals of Maryland* reconheceu que uma determinada interceptação de comunicação era ilícita, porquanto realizada por um particular sem consentimento dos interlocutores ou autorização judicial. Referida conversa captada ilicitamente fora utilizada pela polícia para obter um mandado de busca e apreensão na residência do réu e, quando do cumprimento de tal mandado, a companheira do réu fora questionada pela polícia e informou o local em que aquele escondera a arma do crime e as roupas que utilizara no dia de seu cometimento. A Corte manteve a condenação à pena de morte, pois, embora tenha reconhecido a ilicitude da interceptação e ordenado sua supressão, a arma do crime e outros objetos apreendidos foram admitidos, tendo em vista que a decisão da companheira de cooperar com a polícia atenuou o uso ilegal da comunicação captada ilicitamente. Explica o acórdão que, apesar de a doutrina do *fruit of the poisonous tree* excluir provas obtidas mediante atos ilegais, esta não se aplica se tais provas advêm de uma fonte independente ou se a conexão entre a fonte (no caso concreto, a companheira do réu) e a prova ilícita originária (a captação ilícita da comunicação) se tornar tão tênue a ponto de que a mácula de ilicitude se dissipe. O acórdão invocou o entendimento da Suprema Corte dos Estados Unidos segundo o qual testemunhas não são como armas ou documentos que ficam escondidos da vista da polícia até alguém levantar um sofá ou abrir um armário. Elas, ao contrário, podem oferecer provas de forma absolutamente voluntária, o que, aliás, frequentemente fazem[289].

---

[288] ESTADOS UNIDOS DA AMÉRICA. United States District Court for the District of Utah. United States v. Jones. 364 F. Supp.2d 1303, 1308-09 (D.Utah 2005). Disponível em: <http://www.lexisnexis.com/hottopics/lnacademic/?>. Acesso em: 12 fev. 2013: "Mr. Jones' email communications (both those originally obtained by the informant and those derivative communications subsequently obtained pursuant to the search warrant) may not be suppressed because § 2515 does not apply to electronic communications, and there is no other applicable suppression remedy under the Wiretap Act. Additionally, because the informant in this case did not intercept any wire or oral communication of Mr. Jones' password (or other information used to access his email account) by means of some device, Mr. Jones' motion to suppress evidence pursuant to the Wiretap Act IS HEREBY DENIED."

[289] ESTADOS UNIDOS DA AMÉRICA. Court of Appeals of Maryland. Jody Lee Miles v. State of Maryland. 365 Md. 488; 781 A.2d 787; 2001 Md. LEXIS 614. Disponível em: <http://www.lexisnexis.com/hottopics/lnacademic/?>. Acesso em: 12 fev. 2013: "The doctrine of the 'fruit of the poisonous tree' although it excludes evidence obtained from or as a consequence of lawless official acts does not apply if such evidence is obtained from an independent source, or such connection may have become so attenuated as to dissipate the taint. … In assessing the voluntariness of the witness's conduct under the attenuation doctrine of the exclusionary rule, the Court explained: Witnesses are not like guns or documents which remain hidden from view until one turns over a sofa or opens a filing cabinet. Witnesses can, and often do, come forward and offer evidence entirely of their own volition. And evaluated properly, the degree of free will necessary to dissipate the taint will very likely be found more often in the case of live-witness testimony than other kinds of evidence. … The first factor of the Brown test of attenuation examines the proximity between the

A dita atenuação dos efeitos da ilicitude sobre uma prova derivada é feita através do que o acórdão chamou de *Brown test*, em referência ao raciocínio adotado pela Suprema Corte dos Estados Unidos no caso *Brown v. Illinois*, em que uma confissão colhida durante prisão reconhecidamente ilegal foi reputada válida pelo fato de a polícia ter promovido o chamado *Miranda warnings*, ou seja, por ter advertido o réu de seu direito de permanecer calado, tendo-se tomado em consideração na análise também outros fatores como a proximidade temporal entre o ato ilícito e a obtenção da prova derivada e o propósito e a flagrância da má conduta policial[290].

3.1.8 Encontro fortuito

O *United States Code* (USC) contém dispositivo específico sobre o tratamento a ser dado em caso de encontro fortuito de provas. Está no 18 USC § 2517, que prevê que, sempre que forem encontradas provas de crimes outros que não aqueles especificados na autorização ou aprovação, estas poderão ser encaminhadas para a apuração própria, mediante concordância do juiz com a legalidade da interceptação que as captou[291].

---

time of the initial illegality and the ascertainment of the evidence that a defendant is seeking to suppress. The United States Supreme Court has not set forth any mathematically precise test for determining at what point the taint has been purged by the lapse of time. Intervening factors or acts following the original unlawful conduct, however, should be considered in assessing attenuation."

[290] ESTADOS UNIDOS DA AMÉRICA. Supreme Court of the United States. Brown v. Illinois. 422 U.S. 590; 95 S. Ct. 2254; 45 L. Ed. 2d 416; 1975 U.S. LEXIS 82. Disponível em: <http://www.lexisnexis.com/hottopics/lnacademic/?>. Acesso em: 02 mar. 2013: "The question whether a confession is the product of a free will under *Wong Sun* must be answered on the facts of each case. No single fact is dispositive. The workings of the human mind are too complex, and the possibilities of misconduct too diverse, to permit protection of the Fourth Amendment to turn on such a talismanic test. The *Miranda* warnings are an important factor, to be sure, in determining whether the confession is obtained by exploitation of an illegal arrest. But they are not the only factor to be considered. The temporal proximity of the arrest and the confession, the presence of intervening circumstances, see *Johnson* v. *Louisiana*, 406 U.S. 356, 365 (1972), and, particularly, the purpose and flagrancy of the official misconduct are all relevant. See *Wong Sun* v. *United States*, 371 U.S., at 491. The voluntariness of the statement is a threshold requirement. Cf. 18 U.S.C. § 3501. And the burden of showing admissibility rests, of course, on the prosecution."

[291] 18 USC § 2517. "Authorization for disclosure and use of intercepted wire, oral, or electronic communications … 5) When an investigative or law enforcement officer, while engaged in intercepting wire, oral, or electronic communications in the manner authorized herein, intercepts wire, oral, or electronic communications relating to offenses other than those specified in the order of authorization or approval, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in subsections (1) and (2) of this section. Such contents and any evidence derived therefrom may be used under subsection (3) of this section when authorized or approved by a judge of competent jurisdiction where such judge finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this chapter. Such application shall be made as soon as practicable." (Disponível em: <http://www.law.cornell.edu/uscode/text/18/2517>. Acesso em: 16 fev. 2013).

Há, também, dispositivo específico autorizando o compartilhamento de informações relativas a inteligência ou contrainteligência estrangeira que surjam nas interceptações. Segundo o 18 USC § 2517(6), qualquer oficial de investigação ou procurador que, por qualquer meio, tomar conhecimento do conteúdo de qualquer *wire*, *oral* ou *electronic communication*, ou de prova dele derivada, pode divulgá-lo para qualquer outro oficial de aplicação da lei, inteligência, proteção, imigração, defesa nacional ou segurança nacional na medida em que tal material contiver informações de inteligência ou contrainteligência estrangeira[292].

Verifica-se, ainda, previsão expressa da possibilidade de compartilhamento de comunicações captadas e provas delas decorrentes quando indicarem ameaça de ataque atual ou potencial ou outro tipo de hostilidade de um poder estrangeiro, sabotagem doméstica ou internacional, terrorismo doméstico ou internacional, atividades de reuniões clandestinas de serviços de inteligência ou rede de poderes estrangeiros, com o propósito de prevenir ou responder a tal ameaça[293].

---

[292] 18 USC § 2517. "Authorization for disclosure and use of intercepted wire, oral, or electronic communications … (6) Any investigative or law enforcement officer, or attorney for the Government, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)), or foreign intelligence information (as defined in subsection (19) of section 2510 of this title), to assist the official who is to receive that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information." (Disponível em: <http://www.law.cornell.edu/uscode/text/18/2517>. Acesso em: 16 fev. 2013).

[293] 18 USC § 2517 – "Authorization for disclosure and use of intercepted wire, oral, or electronic communications … (8) Any investigative or law enforcement officer, or other Federal official in carrying out official duties as such Federal official, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents or derivative evidence to any appropriate Federal, State, local, or foreign government official to the extent that such contents or derivative evidence reveals a threat of actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power, domestic or international sabotage, domestic or international terrorism, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by an agent of a foreign power, within the United States or elsewhere, for the purpose of preventing or responding to such a threat. Any official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information, and any State, local, or foreign official who receives information pursuant to this provision may use that information only consistent with such guidelines as the Attorney General and Director of Central Intelligence shall jointly issue." (Disponível em: <http://www.law.cornell.edu/uscode/text/18/2517>. Acesso em: 16 fev. 2013).

3.1.9 Aspectos mais relevantes

Nos Estados Unidos, emana da Quarta Emenda a proteção constitucional à privacidade, cuja aplicabilidade e níveis de incidência serão definidos com base no conceito, segundo a jurisprudência, de *expectation of privacy* que o indivíduo tenha em relação a determinada situação naturalística.

Ao se invocar a *expectation of privacy*, no entanto, os tribunais recorrem ao chamado *Katz test*, que, concebido a partir do caso *Katz v. United States*, se presta a verificar se, sob determinada circunstância, o indivíduo teria uma legítima *expectation of privacy* e se, por outro lado, a sociedade estaria preparada para reconhecer aquela expectativa como razoável.

A *electronic communication*, inserida pela proteção da Quarta Emenda, é doutrinariamente definida como *computer communication*, de modo a diferenciá-la das *oral* e *wire communication*.

A pedido do *prosecutor* ou de alguém por ele designado, um juiz poderá conceder autorização para que se interceptem as *electronic communications*, desde que haja *probable cause* de que o investigado cometeu, esteja cometendo ou esteja prestes a cometer um dos crimes do catálogo que admite a medida.

É possível, como se extrai do teor da exigência acima, a interceptação preventiva, para investigar delito prestes a ser cometido, desde que conste do catálogo.

O referido catálogo, na realidade, é extremamente extenso, porquanto engloba todos os crimes federais.

Outro pressuposto relevante é que procedimentos investigatórios normais tenham sido tentados e falharam ou que tais procedimentos, por sua natureza, sejam incapazes de atingir o objetivo probatório pretendido ou que sejam perigosos demais

Protegem-se, também, as *stored communications*, embora o regime seja diverso e menos rigoroso do que aquele que protege as comunicações em andamento.

A lei exige daquele que requer a interceptação – e isto vemos como um dispositivo concebido para reduzir as chances de que os juízes sejam induzidos a erro –, uma declaração completa dos fatos relativos aos pedidos anteriores de interceptação ou aprovação de interceptação, dirigidos a qualquer juiz envolvendo quaisquer das mesmas pessoas, aparelhos ou locais especificados no pedido, bem como a providência tomada pelo juiz em cada um daqueles casos.

A legislação estabelece o prazo máximo de 30 dias para a medida, mas permite prorrogações por igual período sem que, no entanto, estipule limite de quantas prorrogações podem ser deferidas.

Há previsão de marco temporal preciso a ser considerado como *dies a quo*, qual seja, a manhã do dia em que a interceptação começa a ser executada ou, senão, dez dias depois que a ordem for expedida.

A lei prevê uma forma de interceptação chamada de *roving wiretap*, que se poderia traduzir como "monitoramento itinerante", que não é vinculada ao nome de uma pessoa investigada, mas sim aos equipamentos que esta use ou que se suspeite que venha a usar. O método visa a evitar a frustração da medida através da troca constante de computadores, contas de e-mail ou identidades utilizadas pelo investigado. Diante de controvérsia acerca da possibilidade desse monitoramento indiscriminado de equipamentos, sem uma identificação prévia de *probable cause* em relação a uma determinada pessoa, o que feriria a exigência de individualização da Quarta Emenda, o *Patriot Act* de 2001 veio a ratificar seu cabimento.

As comunicações captadas, bem como as ordens judiciais e pedidos não serão destruídos a menos que haja determinação do juiz, devendo, em qualquer hipótese, ser preservadas por dez anos, mas o acesso pelas partes a esse material não é amplamente assegurado, constando na lei previsão de que o juiz poderá, conforme sua discricionariedade, disponibilizar à pessoa interceptada ou a seu advogado, para inspeção, os trechos das comunicações interceptadas, pedidos e decisões, que ele juiz determinar que sejam do interesse da justiça.

O juiz, portanto, se substitui às partes na verificação dos elementos que a elas poderiam interessar.

Pode ser implementada interceptação sem ordem judicial em caso de emergência que não possa esperar uma autorização, desde que o caso envolva perigo imediato de vida ou de graves danos físicos à pessoa, ou atividades conspiratórias próprias de crime organizado ou que ameacem a segurança nacional. Nesse caso, o investigador deverá apresentar um pedido de aprovação ao juiz dentro de 48 horas.

Também sem ordem judicial poderá ocorrer a interceptação determinada pelo Presidente da República, por períodos de até um ano, para obter informações sobre inteligência estrangeira, desde que não haja risco de se captar comunicação em que uma pessoa dos Estados Unidos seja interlocutora.

Há normas expressas sobre a necessidade de destruir comunicações captadas ilicitamente, mas só se aplicam para as *wire* e *oral communications*, havendo precedente

jurisprudencial invocando este fato para indeferir a supressão de *electronic communication* reputada ilícita.

Verifica-se um tratamento jurisprudencial que classificamos de tolerante com a prova ilícita por derivação, lançando-se mão do chamado *Brown test*, que, tomando em conta fatores como a proximidade temporal entre o ato ilícito originário e a obtenção da prova derivada, bem como o propósito e a flagrância da má conduta policial, permite que se considere dissipada a ilicitude, de modo a não atingir a prova derivada.

O encontro fortuito de prova é amplamente admitido nas interceptações de comunicações, bastando, para a validade da prova, uma autorização do juiz, ao qual bastará verificar se a interceptação que a captou estava regularmente autorizada, nada considerando acerca da conexão dos fatos comprováveis a partir da prova fortuitamente encontrada com os fatos originários.

Ainda mais ampla é a possibilidade de uso da prova fortuitamente encontrada caso ela comprove fatos relativos a inteligência ou contrainteligência estrangeira, ameaça de ataque atual ou potencial ou outro tipo de hostilidade de um poder estrangeiro, sabotagem doméstica ou internacional, terrorismo doméstico ou internacional, atividades de reuniões clandestinas de serviços de inteligência ou rede de poderes estrangeiros. Dizemos mais ampla porque, nessas hipóteses, sequer se exige a autorização do juiz para que se compartilhe a prova.

3.2 Inglaterra

3.2.1 *Right to respect for private and family life*

A Inglaterra não possui uma Constituição *unificada* ou *codificada* ou, ainda, nas palavras de José Afonso da Silva, não possui uma *constituição em sentido forte*[294]. O que é considerada a "Constituição" da Inglaterra é um conjunto de leis, estatutos e atos de grande relevância para a afirmação dos direitos básicos de cidadania[295].

---

[294] SILVA, José Afonso da. **Curso de direito constitucional positivo**. São Paulo: Malheiros, 2010, p. 80.

[295] LAW, David S. **Generic Constitutional Law**. University of San Diego School of Law Public Law and Legal Theory Research Paper Series. paper 23. The Berkeley Electronic Press. 2004. Disponível em: <http://law.bepress.com/cgi/viewcontent.cgi?article=1015&context=sandiegolwps-pllt>. Acesso em: 01.05.2013, p.19/20, 2004: "It is routine to observe that Britain's unwritten 'constitution' includes statutes old

Entre os diversos *acts*, *statutes e settlements* que compõem os textos com caráter constitucional, porém, se encontram textos como a *Magna Cartha* (1215)[296], a *Bill of Rights* (1689)[297], bem como o *Human Rights Act*, de 1998[298].

Observa-se que a *Bill of Rights*, ainda que tenha garantido, por exemplo, a liberdade de expressão e de associação, não traz previsões específicas sobre intimidade ou privacidade, nem sobre inviolabilidade de residência.

A Inglaterra somente passou a contar com positivada proteção à intimidade quando, em 1951, o Reino Unido se tornou signatário da Convenção Europeia de Direitos Humanos[299-300].

A adesão à Convenção, porém, não significou imediata aceitação de todos os seus preceitos, nem tão pouco da jurisdição da Corte Europeia de Direitos Humanos. Esta somente ocorreu em 1960, formalmente, enquanto que a jurisprudência interna do país ainda deixava de aplicar inúmeros preceitos da Convenção sob o discurso de que seriam incompatíveis com o direito britânico, o qual, por sua vez, era soberano. Foi devido a uma campanha agressiva, que uniu juízes e ativistas políticos, que a Convenção veio a ser verdadeiramente internalizada no direito britânico pela promulgação do *Human Rights Act*, em 1998[301], que instrui o Judiciário à adoção da interpretação *pro homine*[302].

Assim, esta lei prevê proteção especial à privacidade e à vida familiar, incluindo, porém, no próprio texto, como cláusulas de exceção, a segurança nacional, a segurança pública ou o

---

and new, from the Habeas Corpus Acts of 1640 and 1679 and the Act of Settlement 1701 to the European Communities Act 1972 and the Human Rights Act 1998."

[296] Disponível em: <http://www.constitution.org/eng/magnacar.htm>. Acesso em: 05 dez. 2013.

[297] The National Archives on behalf of Her Majesty's Government. Her Majesty's Stationery Office (HMSO). Disponível em: <http://www.legislation.gov.uk/aep/WillandMarSess2/1/2/introduction#reference-c1897186>. Acesso em: 02 ago. 2013.

[298] The National Archives on behalf of Her Majesty's Government. Her Majesty's Stationery Office (HMSO). Disponível em: <http://www.legislation.gov.uk/ukpga/1998/42/contents>. Acesso em: 02 ago. 2013.

[299] Disponível em: <http://www.echr.coe.int/Documents/Convention_ENG.pdf>. Acesso em: 02 ago. 2013.

[300] Neste sentido: STAHL, Bernd Carsten. The impact of the UK Human Rights Act 1998 on privacy protection in the workplace. RAMESH, Subramanian (Org.). **Computer Security, Privacy and Politics**: current issues, challenges, and solutions. Hershey: IGI Global, 2008, p. 61/62.

301 EWING, Keith. D. **The Human Rights Act and parliamentary democracy**. Disponível em: <http://onlinelibrary.wiley.com/doi/10.1111/1468-2230.00192/pdf>. Acesso em: 02 jun. 2013: "The Human Rights Act 1998 is the culmination of an aggressive campaign for the incorporation into domestic law of the European Convention on Human Rights, a campaign in which the judges joined forces with other political activists."

[302] Human Rights Act 1998. 2 Interpretation of Convention rights. (1)A court or tribunal determining a question which has arisen in connection with a Convention right must take into account any— (a)judgment, decision, declaration or advisory opinion of the European Court of Human Rights, (b)opinion of the Commission given in a report adopted under Article 31 of the Convention, (c)decision of the Commission in connection with Article 26 or 27(2) of the Convention, or (d)decision of the Committee of Ministers taken under Article 46 of the Convention, whenever made or given, so far as, in the opinion of the court or tribunal, it is relevant to the proceedings in which that question has arisen (Disponível em: <http://www.legislation.gov.uk/ukpga/1998/42/section/2>. Acesso em: 20 nov. 2013); e 3 Interpretation of legislation. (1)So far as it is possible to do so, primary legislation and subordinate legislation must be read and given effect in a way which is compatible with the Convention rights (Disponível em: <http://www.legislation.gov.uk/ukpga/1998/42/section/3>. Acesso em: 20 nov. 2013).

bem-estar econômico do país para a prevenção de desordem ou crime, para a proteção da saúde ou da moral ou para a proteção dos direitos e liberdades dos indivíduos[303].

É preciso dizer que, como a previsão de interceptação é anterior à expressa proteção legal à privacidade[304], esta proteção nasce da interpretação judicial dos casos de interceptação, para, somente a partir de 1988, com sua positivação como direito humano, vir a se amparar nas leis infraexaminadas[305].

3.2.2 A evolução da legislação sobre interceptação das comunicações

A Inglaterra conta com uma significativa concentração de câmeras de vigilância por habitantes, uma para 32, havendo, em Londres, a expectativa de que toda a região central da cidade possa ser acompanhada ao vivo em *streaming*[306].

Para o presente trabalho, importa considerar, de seu surgimento até a enorme popularização que atingiu, a rede chamada de internet, que se serve dos elementos *meio* e *infraestrutura* para transportar o elemento *conteúdo*[307].

Publicação oficial da Coroa Inglesa fez observar que, nos últimos 15 anos, o número de 16 milhões de usuários da internet existentes em 1995 aumentou para 1.7 bilhões nos dias de hoje, trazendo à Inglaterra, junto com as tantas oportunidades positivas, riscos decorrentes da

---

[303] Human Rights Act. 1988. Article 8 Right to respect for private and family life. 1.Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others (Disponível em: <http://www.legislation.gov.uk/ukpga/1998/42/schedule/1>. Acesso em: 07 nov. 2013.)

[304] Wireless Telegraphy Act 1949, Interception Communications Act 1985 e Telecommunications Act 1984

305 EWING, Keith. D. **The Human Rights Act and parliamentary democracy**. Disponível em: <http://onlinelibrary.wiley.com/doi/10.1111/1468-2230.00192/pdf>. Acesso em: 02 jun. 2013.

[306] *Streaming* é um tipo de transmissão de dados *on-line* em que o usuário acessa ao vídeo/áudio "ao vivo" na rede sem necessidade de realizar download de aplicativo para ter acesso ao material (WU, Dapeng. **Streaming video over the internet**: approaches and directions. IEEExplore digital Library. mar. 2011. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=911156>. Acesso em: 05 abr. 2013, p. 282). Há notícias, também, de que, apesar da super-vigilância, a segurança não aumentou, nem mesmo os crimes foram mais facilmente solucionados (DAVENPORT, Justin. Tens of thousands of CCTV cameras, yet 80% of crime unsolved. **London Evening Standard**. 19 set. 2009. Disponível em: <http://www.standard.co.uk/news/tens-of-thousands-of-cctv-cameras-yet-80-of-crime-unsolved-6684359.html>. Acesso em 23 out. 2013. e EVANS, Ian. Report: London no safer for all its CCTV cameras. **The Christian Science Monitor**. 22 fev. 2012. Disponível em: <http://www.csmonitor.com/World/Europe/2012/0222/Report-London-no-safer-for-all-its-CCTV-cameras>. Acesso em: 18 set. 2013).

[307] Ver item 2.1, *supra*.

dependência crescente desta ferramenta[308].

Enquanto no surgimento da internet esta era considerada uma *terra sem lei*, tempo em que leis gerais, do chamado *mundo off-line*, eram o que havia para ser aplicado ao *mundo on-line*[309], hoje, na Inglaterra, diferentemente do que ocorre noutros países, há todo um sistema de vigilância legalmente estatuído do que se faz na internet, que vai desde uma análise do conteúdo de manifestações até a possibilidade de interceptação[310].

Se, por um lado, essa mesma internet surge como um instrumento de potencialização da liberdade de manifestação, tal liberdade vem com efeitos colaterais, como a rapidez de divulgação de discursos difamatórios, o *bullying*, as manifestações de ódio, a perenização de falsidades e conspirações, os ecos da reprodução incontrolável de qualquer manifestação e a própria diminuição da privacidade[311].

Não é, portanto, nenhum exagero afirmar que há, na Inglaterra, uma verdadeira política de interceptação, que demonstra um caráter acentuadamente persecutório nas terras reais. Para entender melhor esse posicionamento, este capítulo analisará os episódios políticos e jurídicos do que se pode chamar de um verdadeiro estado de vigilância britânico e a regulação específica das interceptações telemáticas.

As leis que versam sobre "comunicação", de modo geral, e sobre "telecomunicação" na Inglaterra vieram por necessidades que transcendem a questão de segurança pública e a regulamentação da interceptação. Observamos que a primeira lei que regula a comunicação via rádio de modo amplo na Inglaterra data do início do século. Foi o *Wireless Telegraphy Act*, de 1904, depois substituído por outro *Act*, de mesmo nome, em 1906. Sua principal funcionalidade era apontar a regulação geral da criação de rádios amadoras e os regimes de frequência.

No posterior *Wireless Telegraphy Act* de 1949, definiu-se a comunicação telegráfica como sendo a emissão ou recebimento, por passagens não proporcionadas por nenhuma

---

[308] REINO UNIDO. **A Strong Britain in an Age of Uncertainty**: The National Security Strategy. Presented to Parliament by the Prime Minister by Command of Her Majesty. London: The Stationery Office, 2010. Disponível em: <http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf?CID=PDF&PLA=furl&CRE=nationalsecuritystrategy>. Acesso em: 18 ago. 2013.

[309] ROWBOTTOM, Jacob H. To Rant, Vent And Converse: Protecting Low Level Digital Speech. **Cambridge Law Journal**. v. 71. Paper No 17/2012. 02 abr. 2012. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2033106>. Acesso em: 07 mar. 2013.

[310] Public Order Act 1986, Malicious Communications Act 1988, Protection from Harassment Act 1997, Communications Act 2003, Wireless Telegraphy Act 1949, Interception of Communications Act 1985, Telecommunications Act 1984, Regulation of Investigatory Powers Act 2000, Electronic Communication Act de 2000 e Communications Act de 2003.

[311] ROWBOTTOM, Jacob H. To Rant, Vent And Converse: Protecting Low Level Digital Speech. **Cambridge Law Journal**. v. 71. Paper No 17/2012. 02 abr. 2012. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2033106>. Acesso em: 07 mar. 2013.

substância material construída ou estabelecida para este propósito, de energia eletromagnética numa frequência que não excedesse três milhões de megaciclos por segundo, prestando-se tal energia a transmitir mensagens, sons e imagens[312].

Na vizinha Irlanda, o Regulamento nº 330 de 1937[313] ao *Wireless Telegraphy Act* de 1926[314] trouxe específica proteção ao segredo de informação transmitida por via radiotelegráfica, estabelecendo que o operador de telegrafia que receber uma mensagem sem autorização para conhecer seu conteúdo deve abster-se de saber ou de permitir que seja conhecido esse conteúdo, sua origem ou destinação, sua existência ou o próprio fato de seu recebimento (exceto em caso de devida autorização do governo ou de um tribunal legal competente).

A influência chegou à Inglaterra no *Wireless Telegraphy Act* de 1949, ao tornar punível a violação do sigilo das comunicações, estendendo-lhe a proteção irlandesa. Nesse sentido, dispôs que, exceto se tiver agido com autorização legal, deveria ser criminalmente punida a pessoa que agisse com fins a obter informações sobre conteúdo, remetente ou destinatário de qualquer mensagem a ela não dirigida[315].

---

[312] Wireless Telegraphy Act 1949. 19 Interpretation. (1)In this Act, except where the context otherwise requires, the expression "wireless telegraphy" means the emitting or receiving, over paths which are not provided by any material substance constructed or arranged for that purpose, of electromagnetic energy of a frequency not exceeding three million megacycles a second, being energy which either— (a)serves for the conveying of messages, sound or visual images (whether the messages, sound or images are actually received by any person or not), or for the actuation or control of machinery or apparatus; or (b) is used in connection with the determination of position, bearing or distance, of for the gaining of information as to the presence, absence, position or motion of any object or any objects of any class, and references to stations for wireless telegraphy and apparatus for wireless telegraphy or wireless telegraphy apparatus shall be construed as references to stations and apparatus for the emitting or receiving as aforesaid of such electro-magnetic energy as aforesaid (Disponível em: <http://www.legislation.gov.uk/ukpga/Geo6/12-13-14/54/section/19>. Acesso em: 12 nov. 2013).

[313] No. 330/1937: Wireless Telegraphy Act, 1926. "15. The licensee shall not use or allow the station to be used for the receipt of messages other than messages intended for receipt thereby or sent for general reception. If any other message is unintentionally received by means of the station the licensee shall not make known or allow to be made known its contents, its origin or destination, or the fact of its receipt to any person (other than a duly authorised officer of the Government of Saorstát Eireann or a competent legal tribunal)" (IRLANDA. Irish Statute Book. Produced by The Office of the Attorney General. Disponível em: <http://www.irishstatutebook.ie/1937/en/si/0330.html>. Acesso em: 14 mai. 2013). Para a história da sequência dos "Wireless Acts" e sua importância para o desenvolvimento do rádio na Europa, HALLETT, Lawrie. The Space Between: Making room for Community Radio. In: GORDON, Janey (Ed.) **Notions Of Community**: A Collection of Community Media Debates and Dilemmas. Bern: International Academic Publishers, 2008, p. 44.

[314] Irish Statute Book. Produced by The Office of the Attorney General. Disponível em: <http://www.irishstatutebook.ie/1926/en/act/pub/0045/print.html>. Acesso em: 02 nov. 2013.

[315] Wireless Telegraphy Act 1949. "5. Misleading messages and interception and disclosure of messages. (1) Any person who— ... (b) otherwise than under the authority of a designated person either— (i) uses any wireless telegraphy apparatus with intent to obtain information as to the contents, sender or addressee of any message (whether sent by means of wireless telegraphy or not of which neither the person using the apparatus nor a person on whose behalf he is acting is an intended recipient, (ii) except in the course of legal proceedings or for the purpose of any report thereof, discloses any information as to the contents, sender or addressee of any such message, being information which would not have come to his knowledge but for the use of wireless telegraphy apparatus by him or by another person, shall be guilty of an offence under this Act" (Disponível em: <http://www.legislation.gov.uk/ukpga/Geo6/12-13-14/54/contents>. Acesso em: 06 jan. 2014).

O mesmo *Act* trouxe, ainda, de certa forma, uma previsão indireta de interceptação ao dispor que o crime estaria excluído se o agente houvesse agido contando com autorização do Secretário de Estado, de um Comissário de Alfândega e Impostos ou de outra pessoa designada pelo Secretário de Estado, se a medida fosse necessária para atender ao interesse da segurança nacional, para prevenir ou detectar um crime, para prevenção contra a desordem, para atender ao interesse no bem-estar econômico ou na segurança pública, para proteger a saúde pública ou para fins de recolhimento de tributos ou outros valores destinados ao Estado[316].

Ou seja, embora sem conter específica regulação sobre os procedimentos a serem tomados pelas autoridades competentes para autorizar uma interceptação, esta versão do *Wireless Telegraphy Act* de 1949 já delimitava o poder investigativo em termos de cabimento e de legitimados a autorizar a medida, trazendo, também, a ideia de que a autorização de interceptação fosse vinculada a um período[317], sem, porém, apresentar, naquele momento, um prazo máximo.

Destarte, é de se notar que, à época, na Inglaterra, a facilidade de se conseguir uma interceptação telegráfica tão somente dependendo de alguma autorização administrativa era grande, uma vez que não era necessária intervenção judicial para tal finalidade.

Essa linha mais "permissiva" à atuação do Executivo na investigação se prolongou pelos tempos. Não por outro motivo, o muito mais elaborado e sistemático *Telecommunications Act* de 1984[318] ainda trazia previsões genéricas sobre interceptação, ou seja, ele tipificava o crime de interceptar ou divulgar o conteúdo de mensagens e estabelecia uma causa de exclusão do crime quando, em caso de interceptação, houvesse uma autorização

---

[316] Wireless Telegraphy Act 1949. "5. Misleading messages and interception and disclosure of messages. (4)A separate authority for the purposes of this section is necessary on grounds falling within this subsection if it is necessary— (a)in the interests of national security; (b)for the purpose of preventing or detecting crime (within the meaning of the Regulation of Investigatory Powers Act 2000) or of preventing disorder; (c)in the interests of the economic well-being of the United Kingdom; (d)in the interests of public safety; (e)for the purpose of protecting public health; (f)for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; or (g)for any purpose (not falling within paragraphs (a) to (f)) which is specified for the purposes of this subsection by regulations made by the Secretary of State. … (7)A separate authority for the purposes of this section must be in writing and under the hand of— (a)the Secretary of State; **[**(aa)in the case of an authority given by the Scottish Ministers (by virtue of provision made under section 63 of the Scotland Act 1998), a member of the Scottish Executive;**]** (b)one of the Commissioners of Customs and Excise; or (c)a person not falling within paragraph (a) or (b) who is designated for the purposes of this subsection by regulations made by the Secretary of State" (Disponível em: <http://www.legislation.gov.uk/ukpga/Geo6/12-13-14/54/section/5>. Acesso em: 05 jan. 2014).

[317] Wireless Telegraphy Act 1949. "5. Misleading messages and interception and disclosure of messages. (8) A separate authority for the purposes of this section may be general or specific and may be given — … (b) for such period, and; (c) …" (Disponível em: <http://www.legislation.gov.uk/ukpga/Geo6/12-13-14/54/contents>. Acesso em: 06 jan. 2014).

[318] No intervalo, houve uma modificação ao Wireless Telegraphy Act em 1967, mas nada que tocasse às interceptações. O mesmo ocorreu com o British Telecommunication Act de 1981.

expedida pelo Secretário de Estado ou, em caso de divulgação, esta se desse para instruir investigação criminal[319]. Noutras palavras, tem-se que a divulgação de material interceptado independia de autorização do Secretário de Estado se fosse dirigida para finalidades investigatórias criminais.

O diploma legal trazia uma definição de telecomunicação que ainda estava muito distante da ideia de telemática[320], mas os parâmetros de interceptação acima analisados contribuem em alguma medida com o presente trabalho.

Ideologicamente, porém, é preciso situar a referida lei. Sua aprovação açodada foi fruto de pressões compatíveis com o momento político da eleição do Governo Thatcher em 1983. Primeiramente, o recém-eleito governo conservador carregava o compromisso público de privatizar os serviços de telecomunicações estatais, para o que se tornou necessária a aprovação do *Telecommunications Act* de 1984, que foi, portanto, logo enviado ao Parlamento. Durante os debates legislativos, surgiu uma preocupação geral com a ideia de que, uma vez privatizado o setor, as medidas de interceptação de comunicações, atividade eminentemente estatal, dependeriam da manipulação ou da colaboração de particulares, inexistindo a previsão de mecanismos de controle e disciplina legal para tanto. Foi assim que a Câmara dos Lordes aprovou uma emenda especificando as hipóteses nas quais a interceptação poderia ocorrer, mas, diante do receio de não aprovação da lei, travou-se um compromisso político de se retirar a proposta de emenda naquela sessão, colocando-a em votação na sessão seguinte da Câmara dos Comuns[321].

---

[319] Telecommunications Act 1984. "45 Disclosure of messages etc. (1) A person engaged in the running of a public telecommunication system who otherwise than in the course of his duty— (a) intentionally intercepts a message sent by means of that system; or (b) where a message so sent has been intercepted, intentionally discloses to any person the contents of that message, shall be guilty of an offence. (2) A person engaged in the running of a public telecommunication system who otherwise than in the course of his duty intentionally discloses to any person the contents of any statement of account specifying the telecommunication services provided for any other person by means of that system shall be guilty of an offence. (3) Subsection (1) above does not apply to anything done in obedience to a warrant under the hand of the Secretary of State ; and paragraph (b) of that subsection and subsection (2) above do not apply to any disclosure in connection with the investigation of any criminal offence or for the purposes of any criminal proceedings. (4) A person guilty of an offence under this section shall be liable— (a) on summary conviction, to a fine not exceeding the statutory maximum; (b) on conviction on indictment, to a fine" (Disponível em: <http://www.legislation.gov.uk/ukpga/1984/12/pdfs/ukpga_19840012_en.pdf>. Acesso em: 06 jan. 2014).

[320] Telecommunications Act 1984. "4. Meaning of 'telecommunication system' and related expressions (1)In this Act "telecommunication system" means a system for the conveyance, through the agency of electric, magnetic, electro-magnetic, electro-chemical or electromechanical energy, of— (a)speech, music and other sounds; (b)visual images; (c)signals serving for the impartation (whether as between persons and persons, things and things or persons and things) of any matter otherwise than in the form of sounds or visual images ; or (d)signals serving for the actuation or control of machinery or apparatus" (Disponível em: <http://www.legislation.gov.uk/ukpga/1984/12/section/4>. Acesso em: 22 dez. 2013).

[321] LLOYD, Ian James. The Interception of Communications Act 1985. In: **The Modern Law Review**, vol. 49, n. 1, 1986, p. 88. Disponível em: <http://onlinelibrary.wiley.com/doi/10.1111/j.1468-2230.1986.tb01679.x/pdf>. Acesso em: 12 nov. 2013.

O outro fator de pressão foi o julgamento do Reino Unido pela Corte Europeia de Direitos Humanos no caso *Malone vs. The United Kingdom.* Malone, comerciante de antiguidades, foi processado internamente por comercializar objetos roubados. No curso do julgamento, um policial que prestava depoimento pediu permissão para consultar seu notebook, quando o defensor se apercebeu de que a polícia havia interceptado os telefones do acusado com autorização do Secretário de Administração Interna. Malone não foi condenado no primeiro julgamento, mas, enquanto aguardava um segundo julgamento, ingressou com uma ação cível pleiteando a declaração de ilicitude da gravação de suas comunicações, tendo seu pedido sido julgado improcedente pela *Chancery Division Court*.

A admissibilidade do caso foi afirmada pela Comissão Europeia de Direitos Humanos, que o submeteu à Corte Europeia. Em agosto de 1984, a Corte decidiu que, na falta de regulamentação das circunstâncias autorizadoras da interceptação, – tal qual exigido pelo artigo 8º da Convenção Europeia – não seria possível reconhecer na interceptação telefônica de Malone fundamentos calcados na lei doméstica[322].

Este, portanto, o contexto histórico em que surgiu, um ano após o *Telecommunications Act* de 1984, o *Interception of Communication Act* de 1985 (IOCA), entrando em vigor em 1986[323].

O IOCA[324], como ficou conhecido, teve um importante papel de delimitação dos poderes de interceptação, definindo, em sua *Section 2 – Warrants for Interception*, qual autoridade administrativa poderia conceder autorização para interceptação em quais situações. Permanece a já consolidada autoridade administrativa do Secretário de Estado, mas as hipóteses de cabimento, quais sejam, o interesse da segurança nacional, a prevenção ou detenção de crime grave e a preservação do bem-estar econômico do Reino Unido (já anteriormente previstas no *Wireless Telegraphy Act* de 1949 e no *Human Rights Act* de 1988) aparecem neste *Act* com nova redação, de modo a representarem verdadeiros limites à possibilidade de interceptação[325].

---

[322] TRIBUNAL EUROPEU DE DIREITOS HUMANOS. Caso Malone vs. The United Kingdom. Disponível em: < http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57533>. Acesso em 07 mai. 2013.

[323] Sobre a relação entre o caso Malone e a negativa repercussão internacional quanto ao desrespeito à privacidade na Inglaterra, REID, S. Alan; RYDER, Nicholas. **For Whose Eyes Only?** A Critique of the United Kingdom's Regulation of Investigatory Powers Act 2000, Information & Communications Technology Law, vol. 10, Iss. 2, 2001, p. 183.

[324] Disponível em: <http://www.legislation.gov.uk/ukpga/1985/56/contents>. Acesso em: 09 abr. 2012.

[325] Interception Communications Act 1985. "2. Warrants for interception. (1)Subject to the provisions of this section and section 3 below, the Secretary of State may issue a warrant requiring the person to whom it is addressed to intercept, in the course of their transmission by post or by means of a public telecommunication system, such communications as are described in the warrant; and such a warrant may also require the person to whom it is addressed to disclose the intercepted material to such persons and in such manner as are described in the warrant. (2)The Secretary of State shall not issue a warrant under this section unless he considers that the

O IOCA também trouxe limites quanto à forma de se promover a interceptação, estabelecendo-se que da autorização deveria constar, obrigatoriamente, o nome da pessoa interceptada ou o endereço do local-alvo de interceptação[326].

A previsão da duração da medida, aparecida pela primeira vez num diploma legal, é tão ampla quanto a previsão genérica da autorização: prazo de dois meses para as interceptações autorizadas previamente pelo Secretário de Estado e de dois dias para as interceptações de urgência, autorizadas por pessoa oficialmente delegada pelo Secretário, podendo, contudo, ambas serem renovadas sob a justificativa de sua necessidade, por mais seis meses ou, sem tal justificativa, por mais um mês[327].

Ao narrar o pano de fundo da aprovação do IOCA, Ian J. Loyd (1986) destaca o tradicional sigilo e a obscuridade dos imprecisos regulamentos administrativos, no lugar de rígidos controles legais, com os quais a polícia ou forças de segurança monitoram as comunicações dos cidadãos britânicos. Diz o autor que as críticas à natureza nebulosa desse sistema só costumam aparecer quando a mídia, por alguma razão, dá publicidade a alegações de abusos[328].

---

warrant is necessary— (a)in the interests of national security; (b)for the purpose of preventing or detecting serious crime; or (c)for the purpose of safeguarding the economic well-being of the United Kingdom. (3)The matters to be taken into account in considering whether a warrant is necessary as mentioned in subsection (2) above shall include whether the information which it is considered necessary to acquire could reasonably be acquired by other means. (4)A warrant shall not be considered necessary as mentioned in subsection (2)(c) above unless the information which it is considered necessary to acquire is information relating to the acts or intentions of persons outside the British Islands. (5)References in the following provisions of this Act to a warrant are references to a warrant under this section" (Disponível em: <http://www.legislation.gov.uk/ukpga/1985/56/pdfs/ukpga_19850056_en.pdf>. Acesso em: 09 abr. 2012).

[326] Interception Communications Act 1985. "3. Scope of warrants. (1)Subject to subsection (2) below, the interception required by a warrant shall be the interception of— (a)such communications as are sent to or from one or more addresses specified in the warrant, being an address or addresses likely to be used for the transmission of communications to or from— (i)one particular person specified or described in the warrant; or (ii)one particular set of premises so specified or described; and (b)such other communications (if any) as it is necessary to intercept in order to intercept communications falling within paragraph (a) above" (Disponível em: <http://www.legislation.gov.uk/ukpga/1985/56/pdfs/ukpga_19850056_en.pdf>. Acesso em 08 abr. 2012).

[327] Interception of Communications Act 1985. "4. Issue and Duration of Warrants. (6)In this section "the relevant period"— (a)in relation to a warrant which has not been renewed, means— (i)if the warrant was issued under subsection (1)(a) above, the period of two months beginning with the day on which it was issued; and (ii)if the warrant was issued under subsection (1)(b) above, the period ending with the second working day following that day; (b)in relation to a warrant which was last renewed within the period mentioned in paragraph (a)(ii) above, means the period of two months beginning with the day on which it was so renewed; and (c)in relation to a warrant which was last renewed at any other time, means— (i)if the instrument by which it was so renewed is endorsed with a statement that the renewal is considered necessary as mentioned in section 2(2)(a) or (c) above, the period of six months beginning with the day on which it was so renewed; and (ii)if that instrument is not so endorsed, the period of one month beginning with that day" (Disponível em: <http://www.legislation.gov.uk/ukpga/1985/56/pdfs/ukpga_19850056_en.pdf>. Acesso em: 09 abr. 2012).

[328] DAHRENDORF, Ralph G. et al. (Ed.) The Interception of Communications Act. In: **The Modern Law Review**. vol. 49, n. 1. London: Stevens & Sons Limited, 1986. Disponível em: <http://heinonline.org/HOL/Page?handle=hein.journals/modlr49&div=2&collection=journals&set_as_cursor=0&men_tab=srchresults&terms=the modern law review|49&type=matchall#102>. Acesso em: 16 abr. 2013, p. 86: "In common with many aspects of British governmental practice the monitoring of its citizen's communications,

Após o *Telecommunications Act* e o *Interception of Communications Act*, que regularam durante bom tempo a matéria geral de telecomunicações e interceptações, veio, no limiar do ano 2000, o *Regulation of Investigatory Powers Act*[329], que, apesar de não ter revogado integralmente o *Interception of Communications Act* de 1985[330], vem a ser, no presente, o principal diploma legal regulador das interceptações das comunicações, incluídas as telemáticas.

3.2.3 A legislação britânica na atualidade

O *Regulation of Investigatory Powers Act 2000*, mais conhecido como RIPA, trouxe nova sistematização às interceptações.

A definição de comunicação eletrônica surge com o *Electronic Communication Act* de 2000[331], complementada em seguida pelo *Communications Act* de 2003[332], podendo ser traduzida como a transmissão pelo uso de energia elétrica, magnética ou eletromagnética de sinais de qualquer descrição de uma pessoa para outra, de uma máquina para outra ou de uma pessoa para uma máquina ou vice-versa, através de uma rede de comunicações eletrônicas ou através de outros meios desde que de uma forma eletrônica.

As hipóteses de cabimento para a expedição de uma autorização para interceptação de

---

whether carried out by the police or by the security forces, has traditionally been conducted under conditions of considerable secrecy being governed by somewhat obscure administrative regulations rather than by precise legal controls. Criticism of the nebulous nature of this system has periodically surfaced, normally in response to media publicity concerning alleged abuses, but it was only this year when two distinct sources of pressure coalesced that a somewhat reluctant government introduced the Bill which on July 25 became the Interception of Communications Act."

[329] Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/contents>. Acesso em: 04 set. 2013.

[330] O Regulation of Investigatory Powers Act 2000 revogou as Sections 1 a 10, 11(3) a (5) e o Schedule 1 (anexo) do Interception of Communications Act 1985, mantendo a vigência dos demais dispositivos. Vide RIPA, Schedule 5. Repeals (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/schedule/5>. Acesso em: 04 set. 2013).

[331] Electronic Communications Act 2000. "15 General interpretation. (1) 'electronic communication' means a communication transmitted (whether from one person to another, from one device to another or from a person to a device or vice versa)— (a)by means of an electronic communications network; or (b)by other means but while in an electronic form" (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/7/section/15#commentary-c1908106>. Acesso em: 12 set. 2013).

[332] Communications Act 2003. "32. Meaning of electronic communications networks and services (1)In this Act "electronic communications network" means— (a)a transmission system for the conveyance, by the use of electrical, magnetic or electro-magnetic energy, of signals of any description; and (b)such of the following as are used, by the person providing the system and in association with it, for the conveyance of the signals— (i)apparatus comprised in the system; (ii)apparatus used for the switching or routing of the signals; and (iii)software and stored data" (Disponível em: <http://www.legislation.gov.uk/ukpga/2003/21/section/32>. Acesso em: 12 set. 2013).

comunicações, tal qual fora instituído pelo *Wireless Telegraphy Act* de 1949 e pelo *Human Rights Act* de 1988, são razões de segurança nacional, para prevenir ou detectar um crime grave e para proteger o bem-estar econômico do Reino Unido, mas a estas o RIPA adicionou a possibilidade de interceptação para, em caso de crime grave ou para preveni-lo, dar cumprimento a acordo internacional de assistência mútua[333].

Vale notar que, na hipótese de proteção ao bem-estar econômico, o RIPA passou a dispor que esta só poderá ocorrer se for voltada para obter informações relativas a atos ou intenções de pessoas fora das Ilhas Britânicas[334].

A autorização inscrita no mandado autorizador da interceptação deverá incluir os atos investigatórios necessários para dar cumprimento ao que estiver expressamente autorizado no mandado, incluindo a interceptação de comunicações nele não identificadas. A autorização deverá ser extensiva, também, aos atos necessários à obtenção de dados de comunicações relacionados ao objeto principal do mandado, bem como aos atos acessórios impostos ao destinatário do mandado para que este consiga dar cumprimento aos seus termos principais[335].

Nota-se, portanto, que a expedição de um mandado pode licitamente autorizar o monitoramento de outras comunicações que o executor da medida venha a entender necessárias à sua investigação, bem como o acesso aos dados de tráfego que entenda igualmente necessários.

O RIPA aumentou a lista de legitimados a requerer autorização para interceptar, podendo hoje sê-lo feito pelo diretor geral do serviço de segurança, pelo chefe do serviço secreto de segurança, pelo diretor da sede de comunicações do governo, pelo diretor geral da Agência de Crime Organizado Grave, pelo diretor geral da Agência Escocesa contra o Crime e as Drogas, pelo comissário de polícia metropolitana, pelo chefe de polícia da Irlanda do

---

[333] RIPA 2000. "5 Interception with a warrant ... (3)Subject to the following provisions of this section, a warrant is necessary on grounds falling within this subsection if it is necessary— (a)in the interests of national security; (b)for the purpose of preventing or detecting serious crime; (c)for the purpose of safeguarding the economic well-being of the United Kingdom; or (d)for the purpose, in circumstances appearing to the Secretary of State to be equivalent to those in which he would issue a warrant by virtue of paragraph (b), of giving effect to the provisions of any international mutual assistance agreement" (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/section/5>. Acesso em: 15 set. 2013).

[334] RIPA 2000. "(5) A warrant shall not be considered necessary on the ground falling within subsection (3)(c) unless the information which it is thought necessary to obtain is information relating to the acts or intentions of persons outside the British Islands" (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/section/5>. Acesso em: 15 set. 2013).

[335] RIPA 2000. "(6) The conduct authorised by an interception warrant shall be taken to include— (a)all such conduct (including the interception of communications not identified by the warrant) as it is necessary to undertake in order to do what is expressly authorised or required by the warrant; (b)conduct for obtaining related communications data; and (c)conduct by any person which is conduct in pursuance of a requirement imposed by or on behalf of the person to whom the warrant is addressed to be provided with assistance with giving effect to the warrant" (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/section/5>. Acesso em: 14 set. 2013).

Norte, pelos chefes de outras polícias mantidas sob a autoridade do *Police (Scotland) Act 1967*[336], pelos comissários da Receita e da Alfândega reais, pelo chefe de inteligência de defesa e pela autoridade central de países ou territórios fora do Reino Unido para fins de tratados internacionais de mútua assistência[337].

Para casos de urgência, há previsão da possibilidade de delegação da prerrogativa de autorização de interceptação. No caso da Escócia, em circunstâncias urgentes, a autorização poderá ser expedida por um membro do Poder Executivo escocês ou por um oficial graduado que conte com permissão do Secretário de Estado para a expedição da autorização ou, ainda, por um oficial graduado quando a autorização for destinada a atender pedido formulado pela autoridade competente de país estrangeiro ou território fora do Reino Unido com base em acordo internacional de mútua assistência. Poderá ser expedida autorização, ainda, em caso de urgência, por um servidor graduado da Casa Civil da Escócia que tenha sido designado pelos ministros escoceses como a pessoa autorizada a expedi-la, devendo, neste caso, nela constar tal circunstância[338].

A autorização deverá nominar ou descrever uma pessoa como alvo da interceptação ou um conjunto único de locais relativos à interceptação autorizada. Deverá, também, conter uma

---

[336] Trata-se de consolidação de diversos atos relativos a forças policiais na Escócia e à execução de mandados nos países fronteiriços da Inglaterra e Escócia (Disponível em: <http://www.legislation.gov.uk/ukpga/1967/77/introduction>. Acesso em: 15 abr. 2013).

[337] RIPA 2000. "Application for issue of an interception warrant. (1)An interception warrant shall not be issued except on an application made by or on behalf of a person specified in subsection (2). (2)Those persons are— (a)the Director-General of the Security Service; (b)the Chief of the Secret Intelligence Service; (c)the Director of GCHQ; (d)the Director General of the Serious Organised Crime Agency; (da)the Director General of the Scottish Crime and Drug Enforcement Agency; (e)the Commissioner of Police of the Metropolis; (f)the Chief Constable of the Royal Ulster Constabulary; (g)the chief constable of any police force maintained under or by virtue of section 1 of the M1Police (Scotland) Act 1967; (h) the Commissioners for Her Majesty's Revenue and Customs; (i)the Chief of Defence Intelligence; (j)a person who, for the purposes of any international mutual assistance agreement, is the competent authority of a country or territory outside the United Kingdom. (3)An application for the issue of an interception warrant shall not be made on behalf of a person specified in [F4paragraph (a), (b), (c), (e), (f), (g), (h), (i) or (j)]F4 subsection (2) except by a person holding office under the Crown" (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/section/6>. Acesso em: 15 abr. 2013).

[338] RIPA 2000. "(1)An interception warrant shall not be issued except— (a)under the hand of the Secretary of State or, in the case of a warrant issued by the Scottish Ministers (by virtue of provision made under section 63 of the Scotland Act 1998), a member of the Scottish Executive; or (b)in a case falling within subsection (2) (a) or (b)], under the hand of a senior official.; or (c)in a case falling within subsection (2)(aa), under the hand of a member of the staff of the Scottish Administration who is a member of the Senior Civil Service and who is designated by the Scottish Ministers as a person under whose hand a warrant may be issued in such a case. (2)Those cases are— (a)an urgent case in which the Secretary of State has himself expressly authorised the issue of the warrant in that case; and (aa)an urgent case in which the Scottish Ministers have themselves (by virtue of provision made under section 63 of the Scotland Act 1998) expressly authorised the use of the warrant in that case and a statement of that fact is endorsed on the warrant; and] (b)a case in which the warrant is for the purposes of a request for assistance made under an international mutual assistance agreement by the competent authorities of a country or territory outside the United Kingdom and either— (i)it appears that the interception subject is outside the United Kingdom; or (ii)the interception to which the warrant relates is to take place in relation only to premises outside the United Kingdom" (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/section/7>. Acesso em: 15 set. 2013).

ou mais relações contendo endereços, números, aparatos ou outros fatores a serem usados para identificar as comunicações a serem captadas[339].

No caso de uma autorização restrita ou no caso de autorização para interceptar comunicação externa[340] durante a sua transmissão, desde que esta se realize através de um sistema de comunicações, ou, ainda, se o Secretário de Estado houver emitido um certificado descrevendo o material interceptado que ele considere que deva ser examinado e manifestando que ele considera tal exame necessário para o interesse da segurança nacional, para prevenir ou detectar um crime ou para assegurar o bem-estar econômico do Reino Unido, fica dispensada a exigência acima, qual seja, a menção, na autorização, do nome ou descrição da pessoa-alvo da medida ou dos locais relativos à interceptação e da lista de endereços, números, aparatos e fatores identificadores das comunicações a serem captadas[341].

No que se refere aos prazos de duração da interceptação e suas renovações, houve significativa mudança desde o IOCA de 1985. Para a leitura, importa compreender o significado do que o diploma legal chama de *relevant period*, que vem a ser o período pelo qual a medida pode perdurar. Em casos urgentes, em que o Secretário de Estado houver pessoalmente permitido a expedição de uma autorização por um oficial graduado, considera-se *relevant period* o prazo de cinco dias úteis a partir do dia da expedição da autorização. Em qualquer outra hipótese, o *relevant period* será de três meses a contar da expedição da autorização ou de sua renovação. Mas, por força do Terrorism Act de 2006, nos casos que

---

[339] RIPA 2000. "8 Contents of warrants. (1)An interception warrant must name or describe either— (a)one person as the interception subject; or (b)a single set of premises as the premises in relation to which the interception to which the warrant relates is to take place. (2)The provisions of an interception warrant describing communications the interception of which is authorised or required by the warrant must comprise one or more schedules setting out the addresses, numbers, apparatus or other factors, or combination of factors, that are to be used for identifying the communications that may be or are to be intercepted. (3)Any factor or combination of factors set out in accordance with subsection (2) must be one that identifies communications which are likely to be or to include— (a)communications from, or intended for, the person named or described in the warrant in accordance with subsection (1); or (b)communications originating on, or intended for transmission to, the premises so named or described" (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/section/8>. Acesso em: 16 set. 2013).

[340] Segundo a Section 20 do Regulation of Investigatory Powers Act 2000, trata-se de comunicação enviada ou recebida de algum ponto fora das Ilhas Britânicas: 20 Interpretation of Chapter - In this Chapter ... "external communication" means a communication sent or received outside the British Islands" (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/section/20>. Acesso em 16 set. 2013).

[341] RIPA 2000. "(4)Subsections (1) and (2) shall not apply to an interception warrant if— (a)the description of communications to which the warrant relates confines the conduct authorised or required by the warrant to conduct falling within subsection (5); and (b)at the time of the issue of the warrant, a certificate applicable to the warrant has been issued by the Secretary of State certifying— (i)the descriptions of intercepted material the examination of which he considers necessary; and (ii)that he considers the examination of material of those descriptions necessary as mentioned in section 5(3)(a), (b) or (c). (5)Conduct falls within this subsection if it consists in— (a)the interception of external communications in the course of their transmission by means of a telecommunication system; and (b)any conduct authorised in relation to any such interception by section 5(6). (6)A certificate for the purposes of subsection (4) shall not be issued except under the hand of the Secretary of State" (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/section/8>. Acesso em: 06 set. 2013).

digam respeito à segurança nacional e ao bem-estar econômico do Reino Unido, o *relevant period* será de seis meses a contar do dia da expedição da autorização ou de sua renovação[342].

A medida deverá cessar após o *relevant period*, podendo ser renovada a qualquer tempo antes de seu término, pelo Secretário de Estado ou por ministros escoceses ou membro do Executivo escocês ou, ainda, por um oficial graduado no caso de interceptação requerida por Estado estrangeiro com base em acordo internacional de assistência mútua em que o local interceptado ou a pessoa-alvo da interceptação estejam fora do Reino Unido[343].

Para a renovação da interceptação, esta deve se mostrar ainda necessária para as finalidades legais, ou seja, para proteção à segurança nacional, prevenção ou detecção de um crime grave, proteção do bem-estar econômico do Reino Unido ou para atender a demanda lastreada em acordo internacional de assistência mútua[344]. Por outro lado, a interceptação pode, a qualquer tempo, ser cancelada pelo Secretário de Estado quando cessar sua necessidade[345]. Deverá cessar, também, quando, na modalidade de interceptação das comunicações de pessoa que esteja ou que se acredite estar no exterior, descubra-se que esta, na realidade, se encontra no Reino Unido, desde que a última renovação da autorização não tenha partido do Secretário de Estado[346].

---

[342] RIPA 2000. "(6)In this section "the relevant period"— (a)in relation to an unrenewed warrant issued in a case falling within section 7(2)(a) under the hand of a senior official, means the period ending with the fifth working day following the day of the warrant's issue; (ab)in relation to an unrenewed warrant which is endorsed under the hand of the Secretary of State with a statement that the issue of the warrant is believed to be necessary on grounds falling within section 5(3)(a) or (c), means the period of six months beginning with the day of the warrant's issue; (b)in relation to a renewed warrant the latest renewal of which was by an instrument endorsed under the hand of the Secretary of State with a statement that the renewal is believed to be necessary on grounds falling within section 5(3)(a) or (c), means the period of six months beginning with the day of the warrant's renewal; and (c)in all other cases, means the period of three months beginning with the day of the warrant's issue or, in the case of a warrant that has been renewed, of its latest renewal" (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/section/9?view=plain>. Acesso em 06 set. 2013). As Subsections 6(ab) e 6(b) foram, respectivamente, inserida e alterada pelo Terrorism Act de 2006 (Disponível em: <http://www.legislation.gov.uk/ukpga/2006/11/section/32/prospective>. Acesso em: 07 set. 2013).

[343] RIPA 2000. "(1)An interception warrant— (a)shall cease to have effect at the end of the relevant period; but (b)may be renewed, at any time before the end of that period, by an instrument under the hand of the Secretary of State or, in the case of a warrant issued by the Scottish Ministers (by virtue of provision made under section 63 of the Scotland Act 1998), a member of the Scottish Executive or, in a case falling within section 7(2)(b), under the hand of a senior official" (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/section/9#commentary-c1992607>. Acesso em 12 set. 2013).

[344] RIPA 2000 "(2)An interception warrant shall not be renewed under subsection (1) unless the Secretary of State believes that the warrant continues to be necessary on grounds falling within section 5(3)" (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/section/9#commentary-c1992607>. Acesso em: 12 set. 2013).

[345] RIPA 2000. "(3)The Secretary of State shall cancel an interception warrant if he is satisfied that the warrant is no longer necessary on grounds falling within section 5(3)" (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/section/9#commentary-c1992607>. Acesso em: 12 set. 2013).

[346] RIPA 2000. "(4)The Secretary of State shall cancel an interception warrant if, at any time before the end of the relevant period, he is satisfied in a case in which— (a)the warrant is one which was issued containing the statement set out in section 7(5)(a) or has been renewed by an instrument containing the statement set out in subsection (5)(b)(i) of this section, and (b)the latest renewal (if any) of the warrant is not a renewal by an instrument under the hand of the Secretary of State, that the person named or described in the warrant as the

Em caso de renovação determinada por oficial graduado, a ordem de renovação deverá declarar que o propósito da renovação é uma solicitação de autoridade estrangeira com fulcro em acordo internacional de assistência mútua e, conforme o caso, que o alvo parece se encontrar fora do Reino Unido, além de que o local-alvo da interceptação cuja renovação se pretenda é fora do Reino Unido[347].

O aspecto acima demonstra que, tal qual ocorre nos Estados Unidos, os mecanismos legais de tutela da intimidade não incidem de forma igual sobre nacionais e estrangeiros. No Brasil, apesar de o *caput* do artigo 5º da Constituição sugerir que o rol por ele encabeçado só seja aplicável "aos brasileiros e aos estrangeiros residentes no País", o STF já afirmou que o estrangeiro, mesmo que não domiciliado no Brasil, não se desqualifica como sujeito de direitos e titular de garantias constitucionais e legais[348].

Na *Section 10*, intitulada *Modification of warrants and certificates*, estão dispostas as prerrogativas e os deveres do Secretário de Estado e das demais pessoas com autoridade para expedir autorizações, para modificar as autorizações e os certificados, seja quando se detectar a necessidade de se ampliar seu alcance[349], seja quando as autorizações e certificados já expedidos se mostrarem não mais necessários em toda a sua extensão[350].

Vislumbra-se nesse ponto uma preocupação do legislador em tratar o afastamento do direito à intimidade e privacidade como excepcional, ou seja, como uma invasão na esfera de direitos individuais que deve ser momentânea e de curta duração.

Vislumbra-se, por outro lado, que o *Terrorism Act* de 2006 veio a ampliar, em casos de

---

interception subject is in the United Kingdom" (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/section/9#commentary-c1992607>. Acesso em: 11 set. 2013).

[347] RIPA 2000. "(5)An instrument under the hand of a senior official that renews an interception warrant must contain— (a)a statement that the renewal is for the purposes of a request for assistance made under an international mutual assistance agreement by the competent authorities of a country or territory outside the United Kingdom; and (b)whichever of the following statements is applicable— (i)a statement that the interception subject appears to be outside the United Kingdom; (ii)a statement that the interception to which the warrant relates is to take place in relation only to premises outside the United Kingdom" (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/section/9#commentary-c1992607>. Acesso em: 09 set. 2013).

[348] BRASIL. Supremo Tribunal Federal. HC 94.016/SP, rel. min. Celso de Mello, 2ª T., j. 16.09.2008, DJe 27.02.2009.

[349] RIPA 2000. "10 Modification of warrants and certificates. (1)The Secretary of State may at any time— (a)modify the provisions of an interception warrant; or (b)modify a section 8(4) certificate so as to include in the certified material any material the examination of which he considers to be necessary as mentioned in section 5(3)(a), (b) or (c)" (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/section/10#commentary-c1992607>. Acesso em: 09 set. 2013).

[350] RIPA 2000. "10 Modification of warrants and certificates. … (2)If at any time the Secretary of State considers that any factor set out in a schedule to an interception warrant is no longer relevant for identifying communications which, in the case of that warrant, are likely to be or to include communications falling within section 8(3)(a) or (b), it shall be his duty to modify the warrant by the deletion of that factor. (3)If at any time the Secretary of State considers that the material certified by a section 8(4) certificate includes any material the examination of which is no longer necessary as mentioned in any of paragraphs (a) to (c) of section 5(3), he shall modify the certificate so as to exclude that material from the certified material" (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/section/10#commentary-c1992607>. Acesso em: 20 set. 2013).

risco à segurança nacional, o rol de pessoas autorizadas a modificar ordens judiciais, estendendo tal possibilidade à pessoa que porta ordem, ou seja, ao investigador[351] e a qualquer outra que ocupe a posição de subordinado deste[352]. A concessão de tal prerrogativa a ninguém menos que o próprio portador da autorização para interceptar importa em conceder carta branca para a ampliação ilimitada da violação ao direito individual. Por óbvio, tal previsão proporciona grande agilidade e eficiência investigatória, porém sacrifica os direitos individuais de forma desmedida.

Ao autorizar a interceptação, o Secretário de Estado deverá verificar se ela é proporcional ao fim a que se destina, devendo ele, em tal verificação, certificar-se de que o resultado pretendido não possa ser razoavelmente obtido por outros meios[353].

3.2.4 O tratamento da prova ilícita

O RIPA dispensa tratamento específico ao material decorrente de interceptação ilegal. Dispõe, nesse sentido, que será inadmissível como elemento de prova o material interceptado através da prática do crime de interceptação não autorizada (RIPA, *Section* 1(1) e (2)) e o

---

[351] Redação anterior ao Terrorism Act 2006: "10 Modification of warrants and certificates. … (6)Subsection (4) shall not authorise the making under the hand of either— (a)the person to whom the warrant is addressed, or (b)any person holding a position subordinate to that person, of any modification of any scheduled parts of an interception warrant" (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/section/10/enacted>. Acesso em: 20 set. 2013). Redação atual: "10 Modification of warrants and certificates. … (6)Subsection (4) authorises the modification of the scheduled parts of an interception warrant under the hand of a senior official who is either— . (a)the person to whom the warrant is addressed, or . (b)a person holding a position subordinate to that person, only if the applicable condition specified in subsection (6A) is satisfied and a statement that the condition is satisfied is endorsed on the modifying instrument. (6A)The applicable condition is— . (a)in the case of an unrenewed warrant, that the warrant is endorsed with a statement that the issue of the warrant is believed to be necessary in the interests of national security; and . (b)in the case of a renewed warrant, that the instrument by which it was last renewed is endorsed with a statement that the renewal is believed to be necessary in the interests of national security" (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/section/10#commentary-c1992607>. Acesso em 20 set. 2013).

[352] Uma vez autorizada, a interceptação poderá ser implementada pela pessoa destinatária do mandado ou por seus assistentes: "11 Implementation of warrants. (1)Effect may be given to an interception warrant either— (a)by the person to whom it is addressed; or (b)by that person acting through, or together with, such other persons as he may require (whether under subsection (2) or otherwise) to provide him with assistance with giving effect to the warrant" (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/section/11#reference-c1056655>. Acesso em 21 set. 2013).

[353] RIPA 2000. "5 Interception with a warrant. (2)The Secretary of State shall not issue an interception warrant unless he believes— (a)that the warrant is necessary on grounds falling within subsection (3); and (b)that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct. … (4)The matters to be taken into account in considering whether the requirements of subsection (2) are satisfied in the case of any warrant shall include whether the information which it is thought necessary to obtain under the warrant could reasonably be obtained by other means" (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/section/5>. Acesso em: 21 set. 2013).

material interceptado a pedido de Estado estrangeiro com base em acordo de cooperação quando o Secretário de Estado, ao atender a solicitação, o fizer sobre pessoas que se encontrem no Reino Unido[354].

Mas se, por um lado, a legislação inglesa dá sinais, na *Section 17*, de que inadmite o uso da prova ilícita, por outro, na *Section 18*, traz exceções tão numerosas que parecem esvaziar a norma protetora do indivíduo. Muitas dessas exceções foram instituídas por leis antiterrorismo. Nesse sentido, não importando o grau de infringência da lei na interceptação de uma comunicação, seu resultado deverá ser admitido quando o material interceptado:

- interessar a casos que tenham por objeto crime de interceptação ilegal ou divulgação ilegal de comunicações ou de dados de tráfego, crime de envio de mensagem falsa ou enganosa que ponha em risco a segurança de uma pessoa, de um navio, aeronave ou veículo, crime de envio de falso pedido de socorro, crime de violação de correspondência ou de retardamento de seu trâmite;

- for relativo a procedimento civil voltado para assegurar o cumprimento de um mandado de interceptação por operadores de serviços de comunicações que se recusem a fazê-lo ou retardem a adoção das medidas necessárias;

- for relativo a reclamações instauradas perante o *Investigatory Powers Tribunal*[355];

- for relativo aos procedimentos de restrições financeiras instituídas pelo *Counter-Terrorism Act 2008*;

- for relativo aos procedimentos em trâmite perante a *Special Immigration Appeals Commission*, competente para apreciar recursos em matéria imigratória,

[354] RIPA 2000. "17. Exclusion of matters from legal proceedings. (1)Subject to section 18, no evidence shall be adduced, question asked, assertion or disclosure made or other thing done in, for the purposes of or in connection with any legal proceedings or Inquiries Act proceedings which (in any manner)— (a)discloses, in circumstances from which its origin in anything falling within subsection (2) may be inferred, any of the contents of an intercepted communication or any related communications data; or (b)tends (apart from any such disclosure) to suggest that anything falling within subsection (2) has or may have occurred or be going to occur. (2)The following fall within this subsection— (a)conduct by a person falling within subsection (3) that was or would be an offence under section 1(1) or (2) of this Act or under section 1 of the Interception of Communications Act 1985; (b)a breach by the Secretary of State of his duty under section 1(4) of this Act" (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/section/17#reference-c1056661>. Acesso em: 22 set. 2013).

[355] Sobre o *Investigatory Powers Tribunal*, ver item 3.2.5.

e perante a *Proscribed Organisations Appeal Commission*, competente para apreciar recursos contra decisões do Secretário de Estado que indefiram pedidos para retirar o gravame de "organização proibida" de determinada entidade[356];

– for relativo às chamadas ordens de controle antiterrorismo ("*control orders*"), instituídas pelo *Prevention of Terrorism Act 2005*, que consistem em medidas cautelares restritivas de direitos dirigidas a pessoas suspeitas de terrorismo, a exemplo de proibição de: usar ou possuir determinados artigos ou substâncias, de exercer determinadas atividades, de comunicação ou contato com determinadas pessoas e de restrições de locomoção. O *Prevention of Terrorism Act 2005* prevê que as ordens de controle que não forem incompatíveis com a Convenção Europeia de Direitos Humanos poderão ser determinadas pelo Secretário de Estado e aquelas que forem dependerão de pronunciamento judicial[357-358].

---

[356] A lista de organizações proibidas está disposta no Terrorism Act 2000 (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/11/schedule/2>. Acesso em: 19 mai 2013).

[357] Prevention of Terrorism Act 2005. "Power to make control orders. (1)In this Act "control order" means an order against an individual that imposes obligations on him for purposes connected with protecting members of the public from a risk of terrorism. (2)The power to make a control order against an individual shall be exercisable— (a)except in the case of an order imposing obligations that are incompatible with the individual's right to liberty under Article 5 of the Human Rights Convention, by the Secretary of State; and (b)in the case of an order imposing obligations that are or include derogating obligations, by the court on an application by the Secretary of State. (3)The obligations that may be imposed by a control order made against an individual are any obligations that the Secretary of State or (as the case may be) the court considers necessary for purposes connected with preventing or restricting involvement by that individual in terrorism-related activity. (4)Those obligations may include, in particular— (a)a prohibition or restriction on his possession or use of specified articles or substances; (b)a prohibition or restriction on his use of specified services or specified facilities, or on his carrying on specified activities; (c)a restriction in respect of his work or other occupation, or in respect of his business; (d)a restriction on his association or communications with specified persons or with other persons generally; (e)a restriction in respect of his place of residence or on the persons to whom he gives access to his place of residence; (f)a prohibition on his being at specified places or within a specified area at specified times or on specified days; (g)a prohibition or restriction on his movements to, from or within the United Kingdom, a specified part of the United Kingdom or a specified place or area within the United Kingdom; (h)a requirement on him to comply with such other prohibitions or restrictions on his movements as may be imposed, for a period not exceeding 24 hours, by directions given to him in the specified manner, by a specified person and for the purpose of securing compliance with other obligations imposed by or under the order; (i)a requirement on him to surrender his passport, or anything in his possession to which a prohibition or restriction imposed by the order relates, to a specified person for a period not exceeding the period for which the order remains in force; (j)a requirement on him to give access to specified persons to his place of residence or to other premises to which he has power to grant access; (k)a requirement on him to allow specified persons to search that place or any such premises for the purpose of ascertaining whether obligations imposed by or under the order have been, are being or are about to be contravened; (l)a requirement on him to allow specified persons, either for that purpose or for the purpose of securing that the order is complied with, to remove anything found in that place or on any such premises and to subject it to tests or to retain it for a period not exceeding the period for which the order remains in force; (m)a requirement on him to allow himself to be photographed; (n)a requirement on him to co-operate with specified arrangements for enabling his movements, communications or other activities to be monitored by electronic or other means; (o)a requirement on him to comply with a demand made in the specified manner to provide information to a specified person in accordance with the demand; (p)a requirement on him to report to a

Este último item mostra que a lei britânica dispôs sobre exceção à regra de exclusão da prova produzida contra a lei interna do país em casos de terrorismo, mas, mais do que isso, a prova, neste caso, será admitida mesmo que haja dupla infringência, ou seja, à lei interna e à Convenção Europeia de Direitos Humanos.

A lei inglesa pune com pena de até dois anos e /ou multa, em processos de rito mais complexo (*conviction on indictment*), e pena de até seis meses e/ou multa, em processos de rito mais simples (*summary conviction*), a conduta do agente dos correios ou do funcionário de empresa provedora de serviços de comunicações que dificultarem o cumprimento de mandado de interceptação[359].

Há, também, para buscar assegurar o cumprimento do mandado, a outorga de uma espécie de poder geral de cautela ao Secretário de Estado, que, por força do RIPA[360], pode lançar mão dos poderes judiciais previstos na *Section 45* do *Court of Session Act 1988*[361],

---

specified person at specified times and places" (Disponível em: <http://www.legislation.gov.uk/ukpga/2005/2/contents>. Acesso em 24 set. 2013).

[358] RIPA 2000. "(1)Section 17(1) shall not apply in relation to— (a)any proceedings for a relevant offence; (b)any civil proceedings under section 11(8); (c)any proceedings before the Tribunal; (d)any proceedings on an appeal or review for which provision is made by an order under section 67(8); (da)any control order proceedings (within the meaning of the Prevention of Terrorism Act 2005) or any proceedings arising out of such proceedings; (db)any financial restrictions proceedings as defined in section 65 of the Counter-Terrorism Act 2008, or any proceedings arising out of such proceedings; (e)any proceedings before the Special Immigration Appeals Commission or any proceedings arising out of proceedings before that Commission; or (f)any proceedings before the Proscribed Organisations Appeal Commission or any proceedings arising out of proceedings before that Commission. ... (12)In this section "relevant offence" means— (a)an offence under any provision of this Act; (b)an offence under section 1 of the Interception of Communications Act 1985; (c)an offence under section 47 or 48 of the Wireless Telegraphy Act 2006; (d)an offence under section 83 or 84 of the Postal Services Act 2000" (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/section/17>. Acesso em: 24 set. 2013).

[359] RIPA 2000. "11 Implementation of warrants. **…** (4)Where a copy of an interception warrant has been served by or on behalf of the person to whom it is addressed on— (a)a person who provides a postal service, (b)a person who provides a public telecommunications service, or (c)a person not falling within paragraph (b) who has control of the whole or any part of a telecommunication system located wholly or partly in the United Kingdom, it shall (subject to subsection (5)) be the duty of that person to take all such steps for giving effect to the warrant as are notified to him by or on behalf of the person to whom the warrant is addressed. … (7)A person who knowingly fails to comply with his duty under subsection (4) shall be guilty of an offence and liable— (a)on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine, or to both; (b)on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum, or to both" (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/section/11#reference-c1056655>. Acesso em: 23 set. 2013).

[360] RIPA 2000. "11 Implementation of warrants. … (8)A person's duty under subsection (4) to take steps for giving effect to a warrant shall be enforceable by civil proceedings by the Secretary of State for an injunction, or for specific performance of a statutory duty under section 45 of the Court of Session Act 1988, or for any other appropriate relief" (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/section/11#reference-c1056655>. Acesso em: 23 set. 2013).

[361] Court of Session Act 1988. "45 Restoration of possession and specific performance. The Court may, on application by summary petition— (a)order the restoration of possession of any real or personal property of the possession of which the petitioner may have been violently or fraudulently deprived; and (b)order the specific performance of any statutory duty, under such conditions and penalties (including fine and imprisonment, where

permitindo-lhe expedir ordens específicas para assegurar o cumprimento de qualquer dever legal, sob pena de medidas coercitivas que lhe parecerem adequadas, incluindo a prisão.

A interceptação ilegal, mencionada no *Wireless Telegraphy Act* de 1949 como mera conduta antijurídica, passou a ser, com o IOCA 1985, tipificada como crime punível com prisão de até dois anos e/ou multa, o que foi mantido com o RIPA 2000[362].

Criminalizou-se, ainda, com o estabelecimento de pena de reclusão de até cinco anos e/ou multa, a conduta do servidor que dá publicidade ou divulga ilegalmente o conteúdo de comunicação interceptada, seus dados acessórios (dados de tráfego) ou mesmo a mera existência de uma autorização de monitoramento[363].

---

consistent with the enactment concerned) in the event of the order not being implemented, as to the Court seem proper" (Disponível em: <http://www.legislation.gov.uk/ukpga/1988/36/section/45>. Acesso em: 26 set. 2013).

[362] RIPA 2000. "1 Unlawful interception. (1)It shall be an offence for a person intentionally and without lawful authority to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of— (a)a public postal service; or (b)a public telecommunication system. (2)It shall be an offence for a person— (a)intentionally and without lawful authority, and (b)otherwise than in circumstances in which his conduct is excluded by subsection (6) from criminal liability under this subsection, to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of a private telecommunication system. … (7)A person who is guilty of an offence under subsection (1) or (2) shall be liable— (a)on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine, or to both; (b)on summary conviction, to a fine not exceeding the statutory maximum" (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/section/1>. Acesso em 26 set. 2013).

[363] RIPA 2000. "19 Offence for unauthorised disclosures. (1)Where an interception warrant has been issued or renewed, it shall be the duty of every person falling within subsection (2) to keep secret all the matters mentioned in subsection (3). (2)The persons falling within this subsection are— (a)the persons specified in section 6(2); (b)every person holding office under the Crown; (c)every member of the staff of the Serious Organised Crime Agency; (ca)every member of the Scottish Crime and Drug Enforcement Agency; (e)every person employed by or for the purposes of a police force; (f)persons providing postal services or employed for the purposes of any business of providing such a service; (g)persons providing public telecommunications services or employed for the purposes of any business of providing such a service; (h)persons having control of the whole or any part of a telecommunication system located wholly or partly in the United Kingdom. (3)Those matters are— (a)the existence and contents of the warrant and of any section 8(4) certificate in relation to the warrant; (b)the details of the issue of the warrant and of any renewal or modification of the warrant or of any such certificate; (c)the existence and contents of any requirement to provide assistance with giving effect to the warrant; (d)the steps taken in pursuance of the warrant or of any such requirement; and (e)everything in the intercepted material, together with any related communications data. (4)A person who makes a disclosure to another of anything that he is required to keep secret under this section shall be guilty of an offence and liable— (a)on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine, or to both; (b)on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum, or to both" (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/section/19>. Acesso em: 24 set. 2013).

3.2.5 *The Investigatory Powers Tribunal*

Ponto diferencial da legislação inglesa, instituído pelo IOCA 1985 (e mantido pelo RIPA 2000), foi a criação de um tribunal especializado para avaliar casos de abuso de interceptação, seja a feita por particulares, seja a feita pelo ente estatal.

Referido Tribunal, chamado de *Investigatory Powers Tribunal*, mostra algumas especificidades como a possibilidade de ser acionado desde o momento da investigação, para apurar a legalidade das autorizações de interceptação e a proibição de recursos, não podendo as suas decisões ser questionadas nem mesmo pela Suprema Corte. Outra peculiaridade é a possibilidade que qualquer pessoa tem de, uma vez suspeitando que o sigilo de suas comunicações tenha sido ou esteja sendo violado, representar ao Tribunal para apurar tal suspeita[364].

Após a instauração de um processo, se procedente o pleito, o Tribunal poderá adotar medidas como a anulação de autorizações de interceptação, a destruição do material arrecadado e a compensação financeira do reclamante[365].

---

[364] Interception of Communications Act 1985. "7. The Tribunal (1)There shall be a tribunal (in this Act referred to as "the Tribunal") in relation to which the provisions of Schedule 1 to this Act shall apply. (2)Any person who believes that communications sent to or by him have been intercepted in the course of their transmission by post or by means of a public telecommunication system may apply to the Tribunal for an investigation under this section. (3)On such an application (other than one appearing to the Tribunal to be frivolous or vexatious), the Tribunal shall investigate— (a)whether there is or has been a relevant warrant or a relevant certificate; and (b)where there is or has been such a warrant or certificate, whether there has been any contravention of sections 2 to 5 above in relation to that warrant or certificate. (4)If, on an investigation, the Tribunal, applying the principles applicable by a court on an application for judicial review, conclude that there has been a contravention of sections 2 to 5 above in relation to a relevant warrant or a relevant certificate, they shall— (a)give notice to the applicant stating that conclusion; (b)make a report of their findings to the Prime Minister; and (c)if they think fit, make an order under subsection (5) below. (5)An order under this subsection may do one or more of the following, namely— (a)quash the relevant warrant or the relevant certificate; (b)direct the destruction of copies of the intercepted material or, as the case may be, so much of it as is certified by the relevant certificate; (c)direct the Secretary of State to pay to the applicant such sum by way of compensation as may be specified in the order. (6)A notice given or report made under subsection (4) above shall state the effect of any order under subsection (5) above made in the case in question. (7)If, on an investigation, the Tribunal come to any conclusion other than that mentioned in subsection (4) above, they shall give notice to the applicant stating that there has been no contravention of sections 2 to 5 above in relation to a relevant warrant or a relevant certificate. (8)The decisions of the Tribunal (including any decisions as to their jurisdiction) shall not be subject to appeal or liable to be questioned in any court. (9)For the purposes of this section— (a)a warrant is a relevant warrant in relation to an applicant if— (i)the applicant is specified or described in the warrant; or (ii)an address used for the transmission of communications to or from a set of premises in the British Islands where the applicant resides or works is so specified; (b)a certificate is a relevant certificate in relation to an applicant if and to the extent that an address used as mentioned in paragraph (a)(ii) above is specified in the certificate for the purpose of including communications sent to or from that address in the certified material" (Disponível em: <http://www.legislation.gov.uk/ukpga/1985/56/section/7/enacted>. Acesso em: 25 set. 2013).

[365] Interception of Communications Act 1985. "7. The Tribunal … (5)An order under this subsection may do one or more of the following, namely— (a)quash the relevant warrant or the relevant certificate; (b)direct the destruction of copies of the intercepted material or, as the case may be, so much of it as is certified by the relevant certificate; (c)direct the Secretary of State to pay to the applicant such sum by way of compensation as

A fama do Tribunal – único no mundo, no que tange, explicitamente, à competência e à ausência de foro recursal[366] – se estendeu por duas razões: pelo fato de suas decisões serem secretas, em virtude da manutenção da "segurança" e por ter, de 2000 a 2009, das 956 interceptações por ele analisadas, julgado apenas quatro ilegais, número patentemente inferior ao esperado em face de um país tão invasivo à intimidade e à privacidade[367].

A regulação do *Investigatory Powers Tribunal* pelo RIPA o institui como o único juízo competente para apreciar questionamentos quanto à violação dos direitos individuais assegurados pelo *Human Rights Act*, que internalizou os termos da Convenção Europeia[368].

3.2.6 Os dados de tráfego

A legislação inglesa diferenciou muito claramente os chamados dados de tráfego dos dados de conteúdo de comunicações, ao definir interceptação como o monitoramento ou interferência no sistema de telecomunicação que torne o conteúdo da comunicação disponível a uma pessoa distinta de seu remetente ou de seu destinatário[369]. Excluída do conceito de

---

may be specified in the order" (Disponível em: <http://www.legislation.gov.uk/ukpga/1985/56/section/7/enacted>. Acesso em: 20 set. 2013).

[366] GILLESPIE, Alisdair. **The English Legal System**. Oxford: Oxford University Press, 2007, p. 45.

[367] Conforme dados do *site* de próprio *Investigatory Powers Tribunal*: "Welcome to the Investigatory Powers Tribunal (IPT) website. The IPT exists to investigate complaints about the potential conduct of various public bodies, in relation to you, your property or communications. This site explains the functions, structure and jurisdiction of the Tribunal and provides contact details should you need further information or wish to make a complaint. The IPT was established in October 2000, as a result of the enactment of the Regulation of Investigatory Powers Act (RIPA, 2000). The IPT can consider complaints about the use of a number of intrusive powers used by intelligence services, law enforcement agencies and public authorities. Biographies of the 9 Tribunal members can be found here This website is intended to provide support to the work of the Tribunal. We are always keen to hear how it can be improved, so please contact us should you have any suggestions" (Disponível em: <http://www.ipt-uk.com/default.asp?sectionID=16>. Acesso em: 06 jul. 2013).

[368] RIPA 2000. "The Tribunal. (1)There shall, for the purpose of exercising the jurisdiction conferred on them by this section, be a tribunal consisting of such number of members as Her Majesty may by Letters Patent appoint. (2)The jurisdiction of the Tribunal shall be— (a)to be the only appropriate tribunal for the purposes of section 7 of the Human Rights Act 1998 in relation to any proceedings under subsection (1)(a) of that section (proceedings for actions incompatible with Convention rights) which fall within subsection (3) of this section; (b)to consider and determine any complaints made to them which, in accordance with subsection (4), are complaints for which the Tribunal is the appropriate forum; (c)to consider and determine any reference to them by any person that he has suffered detriment as a consequence of any prohibition or restriction, by virtue of section 17, on his relying in, or for the purposes of, any civil proceedings on any matter; and (d)to hear and determine any other such proceedings falling within subsection (3) as may be allocated to them in accordance with provision made by the Secretary of State by order" (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/part/IV/crossheading/the-tribunal>. Acesso em 18 set. 2013).

[369] RIPA 2000. "2 Meaning and location of "interception" etc. (2)For the purposes of this Act, but subject to the following provisions of this section, a person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if, he— (a)so modifies or interferes with the system, or its operation, (b)so monitors transmissions made by means of the system, or (c)so monitors transmissions made by

interceptação está, por óbvio, a captação de radiodifusão de recepção geral[370], mas também os dados de tráfego, considerados quaisquer dados que identifiquem as pessoas, os aparelhos ou a localização de onde ou para onde a comunicação esteja sendo transmitida[371].

O regime de proteção aos dados de tráfego é distinto daquele que protege as comunicações em seu conteúdo, o que se extrai da leitura da *Section 22* do RIPA, na qual tais dados são tratados por *communication data*[372]. Chega-se rapidamente a tal conclusão com a leitura da *Subsection* (1) da *Section* 22, que dispõe que qualquer investigador pertencente aos quadros dos órgãos de persecução mencionados no RIPA poderá requisitar dados de tráfego aos prestadores de serviços de comunicações no interesse da segurança nacional, para detectar ou prevenir um crime ou a desordem, para preservar o bem-estar econômico do Reino Unido, para preservar a segurança pública e a saúde pública, para fiscalizar ou cobrar o pagamento de tributos, para, em caso de emergência, prevenir morte ou danos físicos e mentais ou para minorar tais danos ou, ainda, para servir a qualquer finalidade que, embora não prevista neste

---

wireless telegraphy to or from apparatus comprised in the system, as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication" (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/section/2>. Acesso em 28 set. 2013).

[370] RIPA 2000. "2 Meaning and location of "interception" etc. (3)References in this Act to the interception of a communication do not include references to the interception of any communication broadcast for general reception" (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/section/2>. ACesso em 28 set. 2013).

[371] RIPA 2000. "2 Meaning and location of "interception" etc. (5)References in this Act to the interception of a communication in the course of its transmission by means of a postal service or telecommunication system do not include references to— (a)any conduct that takes place in relation only to so much of the communication as consists in any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted; or (b)any such conduct, in connection with conduct falling within paragraph (a), as gives a person who is neither the sender nor the intended recipient only so much access to a communication as is necessary for the purpose of identifying traffic data so comprised or attached. … (9)In this section "traffic data", in relation to any communication, means— (a)any data identifying, or purporting to identify, any person, apparatus or location to or from which the communication is or may be transmitted, (b)any data identifying or selecting, or purporting to identify or select, apparatus through which, or by means of which, the communication is or may be transmitted, (c)any data comprising signals for the actuation of apparatus used for the purposes of a telecommunication system for effecting (in whole or in part) the transmission of any communication, and (d)any data identifying the data or other data as data comprised in or attached to a particular communication, but that expression includes data identifying a computer file or computer program access to which is obtained, or which is run, by means of the communication to the extent only that the file or program is identified by reference to the apparatus in which it is stored" (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/section/2>. Acesso em: 28 set. 2013).

[372] RIPA 2000. "21 Lawful acquisition and disclosure of communications data. ... (4)In this Chapter "communications data" means any of the following— (a)any traffic data comprised in or attached to a communication (whether by the sender or otherwise) for the purposes of any postal service or telecommunication system by means of which it is being or may be transmitted; (b)any information which includes none of the contents of a communication (apart from any information falling within paragraph (a)) and is about the use made by any person— (i)of any postal service or telecommunications service; or (ii)in connection with the provision to or use by any person of any telecommunications service, of any part of a telecommunication system; (c)any information not falling within paragraph (a) or (b) that is held or obtained, in relation to persons to whom he provides the service, by a person providing a postal service or telecommunications service (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/section/21>. Acesso em: 29 set. 2013).

rol, conste de uma ordem proferida pelo Secretário de Estado declarando que a requisição dos dados atenderá, indiretamente, as finalidades previstas no rol legal[373].

Afinal, o rol é significativamente maior do que aquele contendo as hipóteses em que se pode autorizar a interceptação de conteúdo das comunicações (previstas na *Section 5(3)* do RIPA 2000), além de conter uma possibilidade "em branco" concedida ao Secretário de Estado.

3.2.7 Armazenamento obrigatório de dados de tráfego

Em 2009, o Secretário de Estado expediu o Regulamento nº 859, posteriormente aprovado pelas duas Casas Legislativas, dispondo sobre a obrigação dos provedores de serviços de comunicação de armazenar dados de tráfego relativos a conexões de internet, e-mail, telefonia fixa e móvel, telefonia baseada em internet e até mesmo chamadas não atendidas[374], por um prazo de doze meses, a contar do momento da comunicação[375]. O regulamento, no entanto, exclui expressamente a obrigação de retenção de dados de conteúdo de comunicações.

---

[373] RIPA 2000. "22 Obtaining and disclosing communications data. (1)This section applies where a person designated for the purposes of this Chapter believes that it is necessary on grounds falling within subsection (2) to obtain any communications data. (2)It is necessary on grounds falling within this subsection to obtain communications data if it is necessary— (a)in the interests of national security; (b)for the purpose of preventing or detecting crime or of preventing disorder; (c)in the interests of the economic well-being of the United Kingdom; (d)in the interests of public safety; (e)for the purpose of protecting public health; (f)for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; (g)for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health; or (h)for any purpose (not falling within paragraphs (a) to (g)) which is specified for the purposes of this subsection by an order made by the Secretary of State" (Disponível em: http://www.legislation.gov.uk/ukpga/2000/23/section/22>. Acesso em: 29 set. 2013).

[374] RIPA 2000. "Obligation to retain communications data. 4.—(1) It is the duty of a public communications provider to retain the communications data specified in the following provisions of the Schedule to these Regulations— (a)Part 1 (fixed network telephony); (b)Part 2 (mobile telephony); (c)Part 3 (internet access, internet e-mail or internet telephony). (2) The obligation extends to data relating to unsuccessful call attempts that— (a)in the case of telephony data, are stored in the United Kingdom, or (b)in the case of internet data, are logged in the United Kingdom. (3) An "unsuccessful call attempt" means a communication where a telephone call has been successfully connected but not answered or there has been a network management intervention. (4) The obligation does not extend to unconnected calls. (5) No data revealing the content of a communication is to be retained in pursuance of these Regulations" (Disponível em: <http://www.legislation.gov.uk/uksi/2009/859/regulation/4/made>. Acesso em: 29 set. 2013).

[375] The Data Retention (EC Directive) Regulations 2009. "The retention period. 5. The data specified in the Schedule to these Regulations must be retained by the public communications provider for a period of 12 months from the date of the communication in question" (Disponível: <http://www.legislation.gov.uk/uksi/2009/859/regulation/5/made>. Acesso em: 30 set. 2013).

3.2.8 Disciplina legal da criptografia

Observe-se, ainda, que o RIPA trouxe previsão expressa de que, quando o material interceptado estiver ilegível em razão de criptografia, qualquer pessoa que necessitar, na condução legal de uma investigação, do código para violar a criptografia, poderá representar a um juiz[376] pugnando por uma autorização chamada de *appropriate permission*, que concede ao investigador o poder de expedir uma determinação dirigida a quem possui a chave ou senha para que a forneça em prazo determinado[377], sob pena de incorrer em crime de descumprimento de intimação (*Failure to comply with a notice*), com pena de reclusão de até cinco anos (em caso de obscenidades contra crianças) ou de até dois anos (nos demais casos), ou, ainda, de até seis meses em caso de condenação sumária[378].

Impossível não notar a ligação entre a criminalização da recusa em fornecer chave para abrir uma criptografia e o direito de não se autoincriminar. No caso *R v S and another*, os acusados alegaram, perante a *Criminal Division* da *Court of Appeal* da Inglaterra, que sua recusa em fornecer a chave de acesso a material protegido por criptografia foi a base da

---

[376] No caso da Inglaterra e Gales, trata-se de um *circuit judge* ou de um *district judge*; No caso da Escócia, trata-se de um *sheriff*; e, no caso da Irlanda do Norte, trata-se de um *county court judge*: RIPA 2000. "SCHEDULE 2. Persons having the appropriate permission. *Requirement that appropriate permission is granted by a judge.* 1(1)Subject to the following provisions of this Schedule, a person has the appropriate permission in relation to any protected information if, and only if, written permission for the giving of section 49 notices in relation to that information has been granted— (a)in England and Wales, by a Circuit judge or a District Judge (Magistrates' Courts); (b)in Scotland, by a sheriff; or (c)in Northern Ireland, by a county court judge" (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/schedule/2>. Acesso em: 30 set. 2013).

[377] RIPA 2000. "Part III - Investigation of electronic data protected by encryption etc. Power to require disclosure. 49 Notices requiring disclosure. (2)If any person with the appropriate permission under Schedule 2 believes, on reasonable grounds— (a)that a key to the protected information is in the possession of any person, (b)that the imposition of a disclosure requirement in respect of the protected information is— (i)necessary on grounds falling within subsection (3), or (ii)necessary for the purpose of securing the effective exercise or proper performance by any public authority of any statutory power or statutory duty, (c)that the imposition of such a requirement is proportionate to what is sought to be achieved by its imposition, and (d)that it is not reasonably practicable for the person with the appropriate permission to obtain possession of the protected information in an intelligible form without the giving of a notice under this section, the person with that permission may, by notice to the person whom he believes to have possession of the key, impose a disclosure requirement in respect of the protected information" (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/part/III/crossheading/power-to-require-disclosure>. Acesso em: 02 out. 2013).

[378] RIPA 2000. "53 Failure to comply with a notice. (1)A person to whom a section 49 notice has been given is guilty of an offence if he knowingly fails, in accordance with the notice, to make the disclosure required by virtue of the giving of the notice. ... (5)A person guilty of an offence under this section shall be liable— (a)on conviction on indictment, to imprisonment for a term not exceeding the appropriate maximum term or to a fine, or to both; (b)on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum, or to both. (5A)In subsection (5) 'the appropriate maximum term' means— (a)in a national security case or a child indecency case, five years; and (b)in any other case, two years" (Disponível em: <http://www.legislation.gov.uk/ukpga/2000/23/part/III>. Acesso em: 02 out. 2013).

acusação formulada contra eles, o que seria incompatível com o direito contra a autoincriminação, além de afrontar a garantia de processo equitativo assegurada no artigo 6º da Convenção Europeia.

Entendeu a Corte que não houve violação ao direito contra a autoincriminação, pois a senha de acesso buscada pelo Estado, que apenas se prestaria a dar acesso ao material criptografado, tinha existência independente das mentes dos réus, tal qual ocorreria com impressões digitais, amostras de sangue e gravações de voz[379].

3.2.9 Aspectos mais relevantes

Na Inglaterra, os direitos à privacidade e à vida familiar decorrem, de forma mais efetiva, do *Human Rights Act* de 1998, que fez internalizar no país a Convenção Europeia de Direitos Humanos.

A interceptação das *electronic communication* pode ser implementada mediante autorização do Secretário de Estado, por razões de segurança nacional, para prevenir ou detectar um crime grave, para proteger o bem-estar econômico do Reino Unido e para dar

[379] "Neither S nor A complied with the notices. Their position was that the notices which compelled them to disclose the passwords or 'keys' to the encrypted computer files were incompatible with the privilege against self-incrimination. Their refusal formed the basis of the counts in the indictment which Judge Stephens was invited to stay on the basis that 'the requirement to provide information to the police under Pt III of RIPA constituted an impermissible infringement of the . . . privilege against self-incrimination' and contravened art 6 of the European Convention of Human Rights. … Judge Stephens decided that the privilege against self-incrimination was not engaged on the basis that the material in question had a separate existence, independent of the minds of the Appellants, and in any event, that the proposed incursion into the privilege against self-incrimination (if any) was legitimate and proportionate. … The actual answers, that is to say the product of the Appellants' minds could not, of themselves, be incriminating. The keys themselves simply open the locked drawer, revealing its contents. … the keys to them are and remain an independent fact. If however, as for present purposes we are assuming, they contain incriminating material, the fact of the Appellants' knowledge of the keys may itself become an incriminating fact. For example, to know the key to a computer in your possession which contains indecent images of children may itself tend to support the prosecution case that you were knowingly in possession of such material. This was the approach adopted in Re Boucher, a decision of the District Court in Vermont [2007] WL 4246473, where the reasoning acknowledged that some 'acts of production' such as fingerprints, blood samples or voice recordings would not attract the privilege against self-incrimination. … By way of footnote: if the self-incrimination argument was taken as a matter of principle on the basis of legal advice to the Appellants, and they choose, now, to disclose the relevant key, although long out of time, we suspect that the prosecution would be disinclined to proceed with the appropriate counts in the indictment, or if they chose to do so, that the judge would take a merciful view when addressing sentence, at any rate if the protected data turned out to be innocent or simply neutral" (REINO UNIDO. England and Wales Court of Appeal (Criminal Division). R v. S and another. 2008 EWCA Crim 2177; [2008] All ER (D) 89 (Oct). Disponível em: <http://www.lexisnexis.com/lnacui2api/api/version1/getDocCui?lni=4TMY-HYH0-01NS-Y0YD&csi=145262&hl=t&hv=t&hnsd=f&hns=t&hgn=t&oc=00240&perma=true>. Acesso em: 17 jul. 2013).

cumprimento a acordo internacional de assistência mútua, em caso de ocorrência de crime grave ou para preveni-lo.

É permitida, como se vê, a interceptação para fins preventivos, para prevenir crime ou desordem.

Quanto aos legitimados a requerer a medida, o rol é extenso, constando da lei o diretor geral do serviço de segurança, o chefe do serviço secreto de segurança, o diretor da sede de comunicações do governo, o diretor geral da Agência de Crime Organizado Grave, o diretor geral da Agência Escocesa contra o Crime e as Drogas, o comissário de polícia metropolitana, o chefe de polícia da Irlanda do Norte, os chefes de outras polícias mantidas sob a autoridade do *Police (Scotland) Act 1967*, os comissários da Receita e da Alfândega reais, o chefe de inteligência de defesa e a autoridade central de países ou territórios fora do Reino Unido para fins de tratados internacionais de mútua assistência.

As interceptações previamente autorizadas pelo Secretário de Estado poderão perdurar por três meses e aquelas implementadas em casos de urgência, mediante autorização de um oficial graduado indicado pelo Secretário, por cinco dias. Em ambos os casos, é cabível a prorrogação da medida, não tendo a lei estabelecido limite de quantas prorrogações serão possíveis.

Por força do *Terrorism Act* de 2006, no entanto, o prazo da medida será de seis meses nos casos que disserem respeito à segurança nacional e ao bem-estar econômico do Reino Unido.

Há previsão de um poder de modificar autorizações de monitoramento, outorgado basicamente aos mesmos personagens que detêm poder para concedê-las, mas, para casos de risco contra a segurança nacional, o *Terrorism Act* de 2006 ampliou o rol de pessoas detentoras de tal poder, nele incluindo o próprio investigador e qualquer subordinado deste.

A lei inglesa positivou o princípio da proporcionalidade, impondo ao Secretário de Estado que ele, ao apreciar pedido de interceptação, verifique se ela é proporcional ao fim a que se destina, devendo ele se certificar de que o resultado pretendido não possa ser razoavelmente obtido por outros meios.

Há normas inadmitindo o uso de prova ilícita, mas um extenso rol de exceções praticamente esvazia a garantia, estas notadamente voltadas para casos de terrorismo, de violação às normas de imigração e de organizações proibidas.

Peculiaridade no sistema inglês é a existência de um tribunal especializado para avaliar casos de abuso de interceptação, o chamado *The Investigatory Powers Tribunal*, que poderá adotar medidas como a anulação de autorizações de interceptação, a destruição do

material interceptado e a compensação financeira do reclamante. Outra peculiaridade é o fato de que suas decisões não podem ser modificadas por instâncias recursais.

A legislação diferencia os conceitos de dados de tráfego de comunicações do de dados de conteúdo, dando a estes maior proteção. Deu-se, ademais, uma carta branca ao Secretário de Estado quando lhe foi permitido requisitar dados de tráfego, não só em determinadas hipóteses legais, mas também "para servir a qualquer finalidade que, embora não prevista neste rol, conste de uma ordem proferida pelo Secretário de Estado declarando que a requisição dos dados atenderá, indiretamente, as finalidades previstas no rol legal".

Em 2009, estabeleceu-se o armazenamento obrigatório, por um prazo de doze meses, de dados de tráfego relativos a conexões de internet, e-mail, telefonia fixa e móvel, telefonia baseada em internet e até mesmo chamadas não atendidas. O regulamento, no entanto, exclui expressamente a obrigação de retenção de dados de conteúdo de comunicações.

O uso de criptografia é previsto em lei, mas, caso comunicações interceptadas estejam ilegíveis em razão de criptografia, o investigador poderá representar ao juiz pugnando por uma autorização chamada de *appropriate permission*, pela qual ele pode intimar quem possua a chave ou senha de acesso a fornecê-la, sob pena de incorrer em crime de descumprimento de intimação, com pena de reclusão de até cinco anos.

3.3 Espanha

Dona de uma detalhada legislação sobre interceptação de comunicações eletrônicas, a Espanha se apresenta como uma importante fonte de pesquisa a contribuir com o presente trabalho, podendo-se observar, por exemplo, que o país oficializou o dia 28 de janeiro como o *dia de proteção de dados*[380].

[380] "El próximo 28 de enero se celebra el Día de Protección de Datos... que tiene como objetivo principal impulsar el conocimiento entre los ciudadanos europeos de cuáles son sus derechos y responsabilidades en materia de protección de datos, de forma que puedan familiarizarse con un derecho fundamental, que pese a ser menos conocido, está presente en todas las faceta de sus vidas diarias." (ESPANHA. Agencia Española de Protección de Datos, Nota de Prensa. 19 jan. 2010. Disponível em: <https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2010/notas_prensa/common/enero/190110_np_previo_dia_europeo_2010.pdf>. Acesso em: 05 abr. 2013)

3.3.1 Proteção constitucional à intimidade pessoal e familiar e ao segredo das comunicações

A Constituição espanhola assegura o direito à intimidade pessoal e familiar (art. 18.1) e ao segredo das comunicações, em especial as postais, telegráficas e telefônicas, exceto diante de decisão judicial (art. 18.3)[381].

Em comentários ao texto constitucional, Ascensión Elvira Perales (2006) esclarece que, apesar de o artigo 18.3 limitar-se a mencionar as comunicações postais, telegráficas ou telefônicas, deve-se interpretar, dado o caráter aberto do enunciado, que, naquele conceito de comunicações, estão incluídas outras formas comunicativas, a exemplo do correio eletrônico e *chats*, sempre que se efetue por meio de um artifício instrumental ou técnico[382].

Emprega-se, na Espanha[383], o conceito de comunicação em *canal abierto*, exemplificada na Memoria 2010 da Fiscalía, órgão de acusação espanhol, como páginas da *web* de livre acesso, fóruns, *chats* ou grupos de notícias não restritos e servidores FTP, e comunicações em *canal cerrado*, exemplificadas como e-mail, mensagens instantâneas ou qualquer outra forma de comunicação, incluídas aquelas que tenham seu funcionamento típico de *canal abierto* quando se restrinja o livre acesso[384].

---

[381] Constitución española. "Artículo 18. 1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen. ... 3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial" (Dispnível em: <http://www.congreso.es/consti/constitucion/indice/titulos/articulos.jsp?ini=10&fin=55&tipo=2>. Acesso em: 04 nov. 2013).

[382] "Aunque en el artículo 18.3 CE se mencionan sólo las comunicaciones postales, telegráficas o telefónicas, dado el carácter abierto de su enunciado, cabe entender comprendidas otro tipo de comunicaciones como pueda ser el correo electrónico, chats u otros medios, siempre que se efectúen mediante algún artificio instrumental o técnico, pues la presencia de un elemento ajeno a aquéllos entre los que media el proceso de comunicación es indispensable para configurar el ilícito constitucional del precepto." (PERALES, Ascensión Elvira. Sinopsis. Diciembre 2003, Actualizado por Ángeles González Escudero en octubre de 2006. Enero 2011. Disponível em: <http://www.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=18&tipo=2>. Acesso em: 03 nov. 2013).

[383] ESPANHA. Tribunal Supremo. Sala de lo Penal. STS 2756/2008. Recurso 10983/2007. Resolución 249/2008. 28079120012008100290. Ponente: Manuel Marchena Gomez. Fecha: 20/05/2008. Disponível em: <http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=TS&reference=54594&links=&optimize=20080626&publicinterface=true>. Acesso em: 29 mai. 2013: "comunicaciones en canal cerrado, caracterizadas por la expresa voluntad del comunicante de excluir a terceros del proceso de comunicación."

[384] TOURÓN, C. C. P. Memoria elevada al gobierno de s. m. presentada al inicio del año judicial por el Fiscal General del Estado, v. 1. Imprenta Nacional del Boletín Oficial del Estado, Madrid, 2010, p. 1258/1259: "A tal efecto, en el ámbito de las comunicaciones por internet es preciso distinguir entre las que se producen en canal abierto (páginas web de libre acceso, foros, chats o grupos de noticias no restringidos, servidores FTP, etc.) y las que tienen lugar en canal cerrado (correo electrónico, mensajería instantánea, o cualquier otra forma de comunicación, incluidas las mencionadas como propias de canal abierto cuando se restringe el libre acceso). Conforme a lo anteriormente expuesto, únicamente las comunicaciones en canal cerrado están amparadas por el derecho fundamental al secreto de las comunicaciones (art. 18.3 CE) y, en consecuencia, únicamente los datos de tráfico relacionados con las mismas tendrían esa misma consideración."

As comunicações em *canal cerrado* se caracterizam pela vontade do comunicante de excluir terceiros do processo comunicativo, sendo estas, portanto, as únicas compreendidas no âmbito de proteção do artigo 18.3 da Constituição, podendo-se dizer o mesmo em relação ao sigilo sobre os dados de tráfego, que somente estarão protegidos por este dispositivo constitucional quando forem vinculados a comunicações em *canal cerrado*.

O *Tribunal Constitucional de España* já se pronunciou no sentido de que a norma do artigo 18.3 se presta a garantir a impenetrabilidade das comunicações por terceiros, sejam eles públicos ou privados, tendo em vista que o direito ali estabelecido tem eficácia *erga omnes*[385].

Além de o próprio texto do artigo 18.3 excepcionar tais direitos individuais quando diante de decisão judicial, dispõe a mesma Constituição que referidos direitos poderão ser suspensos em razão de estado de exceção, sítio ou alarme (art. 55.1[386]), o que veio a ser regulamentado pela *Ley Orgánica* 4/1981, segundo a qual, na vigência de estado de sítio, exceção ou alarme, o governo poderá interceptar qualquer comunicação, desde que o faça para esclarecimentos de fatos presumivelmente delitivos ou para a manutenção da ordem pública, e desde que se comunique imediatamente ao juiz competente, por escrito e fundamentadamente[387].

Segundo o artigo 116 da Constituição[388], o estado de exceção poderá perdurar por até trinta dias prorrogáveis por igual período, o estado de alarme por até quinze dias prorrogáveis

---

[385] ESPANHA. Tribunal Constitucional de España. Sala Segunda. Recurso de amparo 167/1983. Sentencia 114/1984. Fecha 29/11/1984. disponível em: <http://hj.tribunalconstitucional.es/HJ/pt-BR/Resolucion/Show/SENTENCIA/1984/114>. Acesso em: 30 mai. 2013: "Sea cual sea el ámbito objetivo del concepto de «comunicación», la norma constitucional se dirige inequívocamente a garantizar su impenetrabilidad por terceros (públicos o privados: el derecho posee eficacia *erga omnes*) ajenos a la comunicación misma."

[386] Constitución Española. "Artículo 55. 1. Los derechos reconocidos en los artículos 17, 18, apartados 2 y 3, artículos 19, 20, apartados 1, a) y d), y 5, artículos 21, 28, apartado 2, y artículo 37, apartado 2, podrán ser suspendidos cuando se acuerde la declaración del estado de excepción o de sitio en los términos previstos en la Constitución. Se exceptúa de lo establecido anteriormente el apartado 3 del artículo 17 para el supuesto de declaración de estado de excepción" (Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-1978-31229>. Acesso em: 01 nov. 2013).

[387] Ley Orgánica 4/1981, de 1 de junio, de los estados de alarma, excepción y sitio. "Artículo dieciocho. Uno. Cuando la autorización del Congreso comprenda la suspensión del artículo dieciocho, tres, de la Constitución, la autoridad gubernativa podrá intervenir toda clase de comunicaciones, incluidas las postales, telegráficas y telefónicas. Dicha intervención sólo podrá ser realizada si ello resulta necesario para el esclarecimiento de los hechos presuntamente delictivos o el mantenimiento del orden público. Dos. La intervención decretada será comunicada inmediatamente por escrito motivado al Juez competente" (Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-1981-12774>. Acesso em: 03 nov. 2013).

[388] Constitución española. "Artículo 116. 1. Una ley orgánica regulará los estados de alarma, de excepción y de sitio, y las competencias y limitaciones correspondientes. 2. El estado de alarma será declarado por el Gobierno mediante decreto acordado en Consejo de Ministros por un plazo máximo de quince días, dando cuenta al Congreso de los Diputados, reunido inmediatamente al efecto y sin cuya autorización no podrá ser prorrogado dicho plazo. El decreto determinará el ámbito territorial a que se extienden los efectos de la declaración. 3. El estado de excepción será declarado por el Gobierno mediante decreto acordado en Consejo de Ministros, previa autorización del Congreso de los Diputados. La autorización y proclamación del estado de excepción deberá determinar expresamente los efectos del mismo, el ámbito territorial a que se extiende y su duración, que no

por igual prazo e o estado de sítio poderá perdurar pelo prazo estabelecido pelo Congresso, tendo em vista que é de decretação mais restrita, porquanto de proposta exclusiva do Governo e condicionado à aprovação pela maioria absoluta do Congresso.

Por força do artigo 55.2[389], regulamentado pelo artigo 579.4 da Ley de Enjuiciamiento Criminal (4/1988[390]), o governo poderá, em caso de urgência, suspender o direito ao sigilo das comunicações de quadrilhas armadas e de elementos terroristas, independentemente de ordem judicial, bastando para tanto ordem do Ministro do Interior ou, na falta deste, do Diretor de Segurança do Estado, comunicando-se o fato imediatamente, por escrito e fundamentadamente, ao juiz competente, ao qual caberá manter ou revogar a medida.

Na Espanha, tanto em sua legislação, quanto na jurisprudência, observa-se que um dos métodos constantemente levados em conta para se determinar se uma informação privada está ou não submetida ao direito constitucional ao sigilo das comunicações é a verificação se ela constitui dado interno ou externo a uma comunicação concreta. Os dados internos seriam o conteúdo das comunicações e os externos, também chamados dados de tráfego, são os atinentes a informações outras que não o próprio conteúdo, a exemplo da identificação dos interlocutores, seus endereços, a duração da comunicação, os horários em que conectaram e desconectaram da internet, horários em que conectaram ao servidor de e-mails.

Tal distinção será abordada no item 3.3.2, intitulado "Dados de tráfego e sua preservação obrigatória", mas, desde logo, aponta-se também um critério temporal reconhecido pelo *Tribunal Constitucional de España*, qual seja, o de que o sigilo das comunicações só se presta a proteger comunicações no momento em que elas estejam ocorrendo, pois, a partir de quando o processo comunicativo estiver finalizado ou consumado, os dados decorrentes daquela comunicação estarão protegidos, não mais pelo direito ao sigilo

---

podrá exceder de treinta días, prorrogables por otro plazo igual, con los mismos requisitos. 4. El estado de sitio será declarado por la mayoría absoluta del Congreso de los Diputados, a propuesta exclusiva del Gobierno. El Congreso determinará su ámbito territorial, duración y condiciones" (Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-1978-31229>. Acesso em: 03 nov. 2013).

[389] Constitución Española. "Artículo 55. … 2. Una ley orgánica podrá determinar la forma y los casos en los que, de forma individual y con la necesaria intervención judicial y el adecuado control parlamentario, los derechos reconocidos en los artículos 17, apartado 2, y 18, apartados 2 y 3, pueden ser suspendidos para personas determinadas, en relación con las investigaciones correspondientes a la actuación de bandas armadas o elementos terroristas" (Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-1978-31229>. Acesso em: 03 nov 2013).

[390] Ley de Enjuiciamiento Criminal. "4. En caso de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas o rebeldes, la medida prevista en el número 3 de este artículo podrá ordenarla el Ministro del Interior o en su defecto, el Director de la Seguridad del Estado, comunicándolo inmediatamente por escrito motivado al Juez competente, quien, también de forma motivada, revocará o confirmará tal resolución en un plazo máximo de setenta y dos horas desde que fue ordenada la observación" (Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-1882-6036>. Acesso em 05 nov. 2013).

das comunicações, mas pela norma protetora da intimidade, do artigo 18.1 da Constituição espanhola[391].

3.3.2 A interceptação das comunicações eletrônicas

A chamada *Ley General de Telecomunicaciones* (32/2003) definiu rede de comunicações eletrônicas como um sistema que permita o transporte de sinais mediante cabos, ondas hertzianas, meios óticos e outros meios eletromagnéticos, incluindo redes de satélites e redes terrestres fixas (de comutação de circuitos e pacotes, incluindo a internet) e móveis, sistemas de transmissão elétrica, na medida em que sejam utilizadas para a transmissão de sinais, redes de rádiodifusão sonora e televisiva e rede de TV a cabo[392].

A interceptação legal é definida pelo *Real Decreto* 424/2005 como a medida estabelecida por lei e adotada por uma autoridade judicial que decide ou autoriza o acesso ou a transmissão das comunicações eletrônicas de uma pessoa e a informação relativa à interceptação aos agentes públicos[393].

---

[391] ESPANHA. Tribunal Constitucional de España. Sala Primera. Recurso de amparo 3787-2001. Sentencia 70/2002. Fecha 03/04/2002. Disponível em: <http://hj.tribunalconstitucional.es/HJ/pt/Resolucion/Show/4606>. Acesso em: 30 mai. 2013: "A lo que ha de añadirse otra consideración, relativa al momento en que se produce la intervención policial. Pues tal intervención no interfiere un proceso de comunicación, sino que el citado proceso ya se ha consumado, lo que justifica el tratamiento del documento como tal (como efectos del delincuente que se examinan y se ponen a disposición judicial) y no en el marco del secreto de las comunicaciones. La protección del derecho al secreto de las comunicaciones alcanza al proceso de comunicación mismo, pero finalizado el proceso en que la comunicación consiste, la protección constitucional de lo recibido se realiza en su caso a través de las normas que tutelan la intimidad u otros derechos. Estos dos datos (falta de constancia o evidencia ex ante de que lo intervenido es el objeto de una comunicación secreta impenetrable para terceros y falta de interferencia en un proceso de comunicación) son los decisivos en el presente supuesto para afirmar que no nos hallamos en el ámbito protegido por el derecho al secreto de las comunicaciones postales sino, en su caso, en el ámbito del derecho a la intimidad del art. 18.1 CE. Pues, y esto debe subrayarse, el art. 18.3 CE contiene una especial protección de las comunicaciones, cualquiera que sea el sistema empleado para realizarlas, que se declara indemne frente a cualquier interferencia no autorizada judicialmente."

[392] Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, Anexo II. "25. Red de comunicaciones electrónicas: los sistemas de transmisión y, cuando proceda, los equipos de conmutación o encaminamiento y demás recursos, incluidos los elementos que no son activos que permitan el transporte de señales mediante cables, ondas hertzianas, medios ópticos u otros medios electromagnéticos con inclusión de las redes de satélites, redes terrestres fijas (de conmutación de circuitos y de paquetes, incluida internet) y móviles, sistemas de tendido eléctrico, en la medida en que se utilicen para la transmisión de señales, redes utilizadas para la radiodifusión sonora y televisiva y redes de televisión por cable, con independencia del tipo de información transportada" (Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-2003-20253>. Acesso em 06 nov. 2013).

[393] Real Decreto 424/2005. "Artículo 84. Definiciones. A los efectos de lo dispuesto en este capítulo, los términos definidos en este artículo tendrán el significado siguiente: a) Interceptación legal: medida establecida por ley y adoptada por una autoridad judicial que acuerda o autoriza el acceso o la transmisión de las comunicaciones electrónicas de una persona, y la información relativa a la interceptación, a los agentes

Segundo a *Ley de Enjuiciamiento Criminal*, o juiz poderá determinar o monitoramento de comunicações postais, telegráficas ou telefônicas[394], se este se prestar a viabilizar a descoberta ou comprovação de algum fato ou circunstância importante da causa ou se a medida for promovida sobre as comunicações de pessoa contra a qual haja indícios de responsabilidade criminal[395]. Isto, sem prejuízo da exceção prevista no artigo 579.4 do mesmo diploma, qual seja, da possibilidade de uma interceptação urgente deferida pelo Ministro do Interior ou pelo Diretor de Segurança do Estado, comunicando-se imediatamente ao juiz que, dentro de 72 horas, deverá revogar ou manter o monitoramento[396].

O artigo 33.1 da Ley 32/2003 ratifica a proteção constitucional ao impor aos operadores e prestadores de serviços de comunicações eletrônicas o dever de garantir o segredo das comunicações de seus usuários, mas o artigo 33.2 lhes impõe o dever de viabilizar as interceptações legalmente autorizadas a serem empreendidas pelos agentes públicos que detenham tal atribuição[397].

Observa-se a previsão legal de que os prestadores de serviços de comunicações desenvolvam e mantenham uma interface através da qual o material interceptado será

---

facultados, sin perjuicio de lo establecido en el artículo 579.4 de la Ley de Enjuiciamiento Criminal" (Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-2005-6970>. Acesso em: 05 nov. 2013).

[394] A permissão legal para interceptação se estende também às comunicações eletrônicas, conforme estudo de Ascensión Elvira Perales (2006), referido no item 3.3.1.

[395] Ley de Enjuiciamiento Criminal. "Artículo 579. 1. Podrá el Juez acordar la detención de la correspondencia privada, postal y telegráfica que el procesado remitiere o recibiere y su apertura y examen, si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa. **2.** Asimismo, el Juez podrá acordar, en resolución motivada, la intervención de las comunidades telefónicas del procesado, si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa. **3.** De igual forma, el Juez podrá acordar, en resolución motivada, por un plazo de hasta tres meses, prorrogables por iguales períodos, la observación de las comunicaciones postales, telegráficas o telefónicas de las personas sobre las que existan indicios de responsabilidad criminal, así como de las comunicaciones de las que se sirvan para la realización de sus fines delictivos" (Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-1882-6036>. Acesso em 05 nov. 2013).

[396] Ley de Enjuiciamiento Criminal. "Artículo 579. ... 4. En caso de urgencia, cuando las investigaciones se realicen para la averiguación de delitos relacionados con la actuación de bandas armadas o elementos terroristas o rebeldes, la medida prevista en el número 3 de este artículo podrá ordenarla el Ministro del Interior o, en su defecto, el Director de la Seguridad del Estado, comunicándolo inmediatamente por escrito motivado al Juez competente, quien, también de forma motivada, revocará o confirmará tal resolución en un plazo máximo de setenta y dos horas desde que fue ordenada la observación" (Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-1882-6036>. Acesso em 08 nov. 2013).

[397] Ley 32/2003. "Artículo 33. Secreto de las comunicaciones. 1. Los operadores que exploten redes públicas de comunicaciones electrónicas o que presten servicios de comunicaciones electrónicas disponibles al público deberán garantizar el secreto de las comunicaciones de conformidad con los artículos 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas necesarias. **2**. Los operadores están obligados a realizar las interceptaciones que se autoricen de acuerdo con lo establecido en el artículo 579 de la Ley de Enjuiciamiento Criminal, en la Ley Orgánica 2/2002, de 6 de mayo, Reguladora del Control Judicial Previo del Centro Nacional de Inteligencia y en otras normas con rango de ley orgánica. Asimismo, deberán adoptar a su costa las medidas que se establecen en este artículo y en los reglamentos correspondientes" (Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-2003-20253>. Acesso em: 08 nov. 2013).

transmitido aos centros de recepção das interceptações, ficando o formato de tal interface a cargo de regulamentação do Ministério da Indústria, Turismo e Cultura[398].

Os provedores e operadores deverão viabilizar o monitoramento para todo tipo de comunicações eletrônicas, incluídos os serviços de telefonia e de transmissão de dados, independentemente de se tratar de vídeo, áudio, mensagens, arquivos ou *fac-símile*. Tal viabilização deverá ocorrer mesmo que o investigado se utilize de procedimentos que desviem a chamada a outros serviços de comunicação eletrônica ou a outros terminais, desde que se possa distinguir a comunicação objeto da autorização para monitoramento de outras que não o sejam[399].

A ordem de interceptação poderá determinar aos prestadores de serviços de comunicação, também, além do próprio monitoramento do conteúdo das comunicações, a disponibilização da localização dos interlocutores, do motivo do término da comunicação, da identidade e dados existentes na empresa a respeito do investigado e de seus interlocutores e dos serviços por eles utilizados[400].

---

[398] Ley 32/2003. "Artículo 33. Secreto de las comunicaciones. … 9. Los sujetos obligados deberán tener en todo momento preparadas una o más interfaces a través de las cuales las comunicaciones electrónicas interceptadas y la información relativa a la interceptación se transmitirán a los centros de recepción de las interceptaciones. Las características de estas interfaces y el formato para la transmisión de las comunicaciones interceptadas a estos centros estarán sujetas a las especificaciones técnicas que reglamentariamente se establezcan por el Ministerio de Industria, Turismo y Comercio" (Disponivel em: <http://www.boe.es/buscar/act.php?id=BOE-A-2003-20253>. Acesso em: 09 nov. 2013).

[399] Real Decreto 424/2005. "Artículo 87. Acceso a las comunicaciones electrónicas. … 2. El acceso se facilitará para todo tipo de comunicaciones electrónicas, en particular, por su penetración y cobertura, para las que se realicen mediante cualquier modalidad de los servicios de telefonía y de transmisión de datos, se trate de comunicaciones de vídeo, audio, intercambio de mensajes, ficheros o de la transmisión de facsímil. … 4. El acceso a las comunicaciones se facilitará aun cuando el sujeto de la interceptación utilice procedimientos para desviar las llamadas a otros servicios de comunicaciones electrónicas o a otros puntos de terminación de red, o a otros terminales, y aun cuando las llamadas sean procesadas por proveedores de servicios de comunicaciones electrónicas distintos de aquel al que se dirige la orden de interceptación, siempre que se pueda discernir la comunicación que es objeto de la orden de interceptación" (Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-2005-6970>. Acesso em: 09 nov. 2013).

[400] Real Decreto 424/2005. "Artículo 88. Información relativa a la interceptación. 1. Los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición y sin perjuicio de otros datos que puedan ser establecidos mediante real decreto, los datos indicados en la orden de interceptación legal, de entre los que se relacionan a continuación: a) Identidad o identidades -en la acepción definida en el artículo 84.i)- del sujeto objeto de la medida de la interceptación. b) Identidad o identidades -en la acepción definida en el artículo 84.i)- de las otras partes involucradas en la comunicación electrónica. c) Servicios básicos utilizados. d) Servicios suplementarios utilizados. e) Dirección de la comunicación. f) Indicación de respuesta. g) Causa de finalización. h) Marcas temporales. i) Información de localización. j) Información intercambiada a través del canal de control o señalización. 2. Además de la información relativa a la interceptación prevista en el apartado anterior, los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición y sin perjuicio de otros datos que puedan ser establecidos mediante real decreto, de cualquiera de las partes que intervengan en la comunicación que sean clientes del sujeto obligado, los siguientes datos: a) Identificación de la persona física o jurídica. b) Domicilio en el que el proveedor realiza las notificaciones. Y, aunque no sea abonado, si el servicio de que se trata permite disponer de alguno de los siguientes: c) Número de titular de servicio (tanto el número de directorio como todas las identificaciones de comunicaciones electrónicas del abonado). d) Número de identificación del terminal. e) Número de cuenta asignada por el proveedor de servicios internet. f) Dirección de correo electrónico. 3. Junto

Observa-se na legislação uma preocupação com a adequada conservação do material interceptado, preservando-se sua autenticidade, confidencialidade e integridade. Está no artigo 97 do *Real Decreto* 424/2005, que impõe a adoção de "*todos los medios necesarios para impedir la manipulación de los mecanismos de interceptación, y para garantizar la autenticidad, confidencialidad e integridad de la información obtenida con la interceptación*" [401].

O prazo da medida será aquele fixado na própria autorização, não havendo, no *Real Decreto* 424/2005, previsão de prazo máximo. O artigo 99.3 dispõe apenas que o agente investigador precisará ser notificado pelo prestador de serviço comunicativo do momento em que o mecanismo de interceptação for ativado[402].

Há, no entanto, previsão de prazo de três meses para a medida prorrogáveis por igual período na *Ley de Enjuiciamiento Criminal*[403] e na *Ley Orgánica reguladora del control judicial previo del Centro Nacional de Inteligencia* (2/2002). No caso desta última, que é a agência de inteligência espanhola[404], a autorização deverá ser pedida ao *Tribunal Supremo*,

---

con los datos previstos en los apartados anteriores, los sujetos obligados deberán facilitar, salvo que por las características del servicio no esté a su disposición, información de la situación geográfica del terminal o punto de terminación de red origen de la llamada, y de la del destino de la llamada. En caso de servicios móviles, se proporcionará una posición lo más exacta posible del punto de comunicación y, en todo caso, la identificación, localización y tipo de la estación base afectada" (Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-2005-6970>. Acesso em: 10 nov. 2013).

[401] Real Decreto 424/2005. "Artículo 97. Secreto de las comunicaciones. Las comunicaciones y la información relativa a la interceptación sólo se facilitarán al agente facultado. Para ello, los sujetos a los que se refiere el artículo 85 pondrán todos los medios necesarios para impedir la manipulación de los mecanismos de interceptación, y para garantizar la autenticidad, confidencialidad e integridad de la información obtenida con la interceptación" (Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-2005-6970>. Acesso em: 10 nov. 2013).

[402] Real Decreto 424/2005. "Artículo 99. Plazo de ejecución de la interceptación. 1. El plazo de ejecución de una orden de interceptación legal será el fijado en ella. Cuando no se establezca plazo, las órdenes se ejecutarán antes de las 12:00 horas del día laborable siguiente al que el sujeto obligado reciba la orden de interceptación legal. … **3.** La activación del mecanismo de interceptación será notificada al agente facultado por el medio que se acuerde entre dicho agente y el sujeto obligado" (Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-2005-6970>. Acesso em: 15 nov. 2013).

[403] Ley de Enjuiciamiento Criminal. "Artículo 579. ... 2. Asimismo, el Juez podrá acordar, en resolución motivada, la intervención de las comunidades telefónicas del procesado, si hubiere indicios de obtener por estos medios el descubrimiento o la comprobación de algún hecho o circunstancia importante de la causa. **3.** De igual forma, el Juez podrá acordar, en resolución motivada, por un plazo de hasta tres meses, prorrogables por iguales períodos, la observación de las comunicaciones postales, telegráficas o telefónicas de las personas sobre las que existan indicios de responsabilidad criminal, así como de las comunicaciones de las que se sirvan para la realización de sus fines delictivos" (Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-1882-6036>. Acesso em 05 nov. 2013).

[404] Pelo próprio cabeçalho da lei que criou o Centro Nacional de Inteligencia, pode-se perceber tratar-se de uma agência governamental de inteligência, como a CIA americana, o MI5 inglês, a KGB soviética e, no Brasil, a ABIN (cujos membros se queixam da ausência de permissão legal ou constitucional para promover interceptação de comunicações. Ver item 4.6). Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia. "Artículo 1. El Centro Nacional de Inteligencia. El Centro Nacional de Inteligencia es el Organismo público responsable de facilitar al Presidente del Gobierno y al Gobierno de la Nación las informaciones, análisis, estudios o propuestas que permitan prevenir y evitar cualquier peligro, amenaza o agresión contra la independencia o integridad territorial de España, los intereses nacionales y la estabilidad del Estado de derecho y

mencionando-se as pessoas (se conhecidas) a serem alvo da medida e os locais em que esta se realizará[405].

Mas as investigações conduzidas pela dita agência de inteligência não têm por objeto a investigação de crimes, mas sim os temas próprios de agências governamentais de inteligência, a exemplo, tal qual elencado no artigo 4º da *Ley* 11/2002, de obter e avaliar informações para proteger os interesses políticos, nacionais, econômicos, industriais, comerciais e estratégicos da Espanha, podendo atuar, inclusive, fora do território nacional[406].

---

sus instituciones" ((Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-2002-8628>. Acesso em: 11 nov. 2013).

[405] Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia. "Artículo único. Control judicial previo del Centro Nacional de Inteligencia. 1. El Secretario de Estado Director del Centro Nacional de Inteligencia deberá solicitar al Magistrado del Tribunal Supremo competente, conforme a la Ley Orgánica del Poder Judicial, autorización para la adopción de medidas que afecten a la inviolabilidad del domicilio y al secreto de las comunicaciones, siempre que tales medidas resulten necesarias para el cumplimiento de las funciones asignadas al Centro. 2. La solicitud de autorización se formulará mediante escrito que contendrá los siguientes extremos: a) Especificación de las medidas que se solicitan. b) Hechos en que se apoya la solicitud, fines que la motivan y razones que aconsejan la adopción de las medidas solicitadas. c) Identificación de la persona o personas afectadas por las medidas, si fueren conocidas, y designación del lugar donde hayan de practicarse. d) Duración de las medidas solicitadas, que no podrá exceder de veinticuatro horas en el caso de afección a la inviolabilidad del domicilio y tres meses para la intervención o interceptación de las comunicaciones postales, telegráficas, telefónicas o de cualquier otra índole, ambos plazos prorrogables por sucesivos períodos iguales en caso de necesidad" (Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-2002-8627>. Acesso em: 05 nov. 2013).

[406] Ley 11/2002. "Artículo 4. Funciones del Centro Nacional de Inteligencia. Para el cumplimiento de sus objetivos, el Centro Nacional de Inteligencia llevará a cabo las siguientes funciones: a) Obtener, evaluar e interpretar información y difundir la inteligencia necesaria para proteger y promover los intereses políticos, económicos, industriales, comerciales y estratégicos de España, pudiendo actuar dentro o fuera del territorio nacional. b) Prevenir, detectar y posibilitar la neutralización de aquellas actividades de servicios extranjeros, grupos o personas que pongan en riesgo, amenacen o atenten contra el ordenamiento constitucional, los derechos y libertades de los ciudadanos españoles, la soberanía, integridad y seguridad del Estado, la estabilidad de sus instituciones, los intereses económicos nacionales y el bienestar de la población. c) Promover las relaciones de cooperación y colaboración con servicios de inteligencia de otros países o de Organismos internacionales, para el mejor cumplimiento de sus objetivos. d) Obtener, evaluar e interpretar el tráfico de señales de carácter estratégico, para el cumplimiento de los objetivos de inteligencia señalados al Centro. e) Coordinar la acción de los diferentes organismos de la Administración que utilicen medios o procedimientos de cifra, garantizar la seguridad de las tecnologías de la información en ese ámbito, informar sobre la adquisición coordinada de material criptológico y formar al personal, propio o de otros servicios de la Administración, especialista en este campo para asegurar el adecuado cumplimiento de las misiones del Centro. f) Velar por el cumplimiento de la normativa relativa a la protección de la información clasificada. g) Garantizar la seguridad y protección de sus propias instalaciones, información y medios materiales y personales" (Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-2002-8628:. Acesso em 26 set. 2013).

3.3.3 Dados de tráfego e sua preservação obrigatória

No caso 114/1984, o Tribunal Constitucional afirmou que o "*segreto de las comunicaciones*" assegurado no artigo 18.3 não cobre somente o conteúdo da comunicação, mas também outros aspectos como a identidade dos interlocutores[407].

Anos mais tarde, em 2002, noutro precedente judicial do mesmo Tribunal Constitucional, reconheceu-se que os dados de tráfego (na espécie, tratava-se de dados reveladores do telefone de destino, hora e duração da comunicação) dependem de uma interferência no processo de comunicação e que, por isso, estariam compreendidos no direito ao sigilo das comunicações assegurado no artigo 18.3 da Constituição espanhola. Mais precisamente, afirmou a Corte que tais dados integram o processo comunicativo em sua vertente externa e são confidenciais, ou seja, reservados do conhecimento público e geral, porquanto pertencentes à própria esfera privada dos comunicantes. No entanto, a Corte observou que, apesar disto, não se poderia negar que o acesso aos dados de tráfego relativos à comunicação de um indivíduo ocasiona violação ao direito constitucional ao sigilo das comunicações em menor intensidade do que o ocasionaria a captação do conteúdo de uma comunicação[408].

Mas a matéria foi revista pelo Judiciário Espanhol, havendo precedente mais recente, de 2006, em que o *Tribunal Constitucional de España* restringiu o âmbito de proteção do

---

[407] ESPANHA. Tribunal Constitucional de España. Sala Segunda. Recurso de amparo 167/1983. Sentencia 114/1984. Fecha 29/11/1984. disponível em: <http://hj.tribunalconstitucional.es/HJ/pt-BR/Resolucion/Show/SENTENCIA/1984/114>. Acesso em: 30 mai. 2013: "el concepto de secreto que aparece en el art. 18.3, no cubre sólo el contenido de la comunicación, sino también, en su caso, otros aspectos de la misma, como la identidad subjetiva de los interlocutores o de los corresponsales."

[408] ESPANHA. Tribunal Constitucional de España. Sala Primera. Recurso de amparo 5546/1999. Sentencia 123/2002. Fecha 20/05/2002. Disponível em: <http://hj.tribunalconstitucional.es/HJ/pt/Resolucion/Show/4659>. Acesso em 30 mai. 2013: "la entrega de los listados por las compañías telefónicas a la policía sin consentimiento del titular del teléfono requiere resolución judicial, pues la forma de obtención de los datos que figuran en los citados listados supone una interferencia en el proceso de comunicación que está comprendida en el derecho al secreto de las comunicaciones telefónicas del art. 18.3 CE. En efecto, los listados telefónicos incorporan datos relativos al teléfono de destino, el momento en que se efectúa la comunicación y a su duración, para cuyo conocimiento y registro resulta necesario acceder de forma directa al proceso de comunicación mientras está teniendo lugar, con independencia de que estos datos se tomen en consideración una vez finalizado aquel proceso a efectos, bien de la lícita facturación del servicio prestado, bien de su ilícita difusión. Dichos datos configuran el proceso de comunicación en su vertiente externa y son confidenciales, es decir, reservados del conocimiento público y general, además de pertenecientes a la propia esfera privada de los comunicantes. El destino, el momento y la duración de una comunicación telefónica, o de una comunicación a la que se accede mediante las señales telefónicas, constituyen datos que configuran externamente un hecho que, además de carácter privado, puede asimismo poseer un carácter íntimo. Ahora bien, aunque el acceso y registro de los datos que figuran en los listados constituye una forma de afectación del objeto de protección del derecho al secreto de las comunicaciones, no puede desconocerse la menor intensidad de la injerencia en el citado derecho fundamental que esta forma de afectación representa en relación con la que materializan las "escuchas telefónicas", siendo este dato especialmente significativo en orden a la ponderación de su proporcionalidad."

artigo 18.3 da Constituição aos aspectos da comunicação que fossem ligados à própria condição humana[409], ou seja, restringiu ao conteúdo da mensagem, ao teor que, por um ato humano de vontade, um interlocutor desejou enviar ao outro, excluindo-se, portanto, os dados de tráfego do âmbito de proteção do sigilo das comunicações.

No ano seguinte, em 2007, o Tribunal Constitucional voltou a afirmar que a identidade subjetiva dos interlocutores estaria abarcada pelo âmbito de proteção do artigo 18.3 e que, portanto, o conhecimento destes dependeria de ordem judicial[410].

Em 2008, o *Tribunal Supremo*, apesar de ter reconhecido o caráter acessório dos dados de tráfego, abordou, no caso 2756/2008[411], o debate existente acerca de eles merecerem ou

---

[409] ESPANHA. Tribunal Constitucional de España. Sala Primera. Recurso de amparo 1829-2003. Sentencia 281/2006. Fecha 09/10/2006. Disponível em: <http://hj.tribunalconstitucional.es/HJ/pt/Resolucion/Show/5883>. Acesso em: 30 mai. 2013: "las comunicaciones comprendidas en este derecho han de ser aquellas indisolublemente unidas por naturaleza a la persona, a la propia condición humana; por tanto, la comunicación es a efectos constitucionales el proceso de transmisión de expresiones de sentido a través de cualquier conjunto de sonidos, señales o signos."

[410] ESPANHA. Tribunal Constitucional de España. Sala Primera. Recurso de amparo 6409/2004. Sentencia 230/2007. Fecha 05/11/2007. Disponível em: <http://hj.tribunalconstitucional.es/HJ/pt/Resolucion/Show/6197>. Acesso em: 29 mai. 2013: "conforme a la jurisprudencia establecida por el Tribunal Constitucional, el concepto del secreto de las comunicaciones cubre no sólo el contenido de la comunicación, sino también la identidad subjetiva de los interlocutores, por lo que era exigible, en defecto de prestación del consentimiento, la debida autorización judicial para acceder al listado de llamadas de los teléfonos móviles intervenidos."

[411] ESPANHA. Tribunal Supremo. Sala de lo Penal. STS 2756/2008. Recurso 10983/2007. Resolución 249/2008. 28079120012008100290. Ponente: Manuel Marchena Gomez. Fecha: 20/05/2008. Disponível em: <http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=TS&reference=54594&links=&optimize=20080626&publicinterface=true>. Acesso em: 29 mai. 2013: "A partir de esos datos, resulta obligado plantearse si la numeración IMSI, ajena al contenido de la comunicación propiamente dicho, encierra una información adicional que, pese a su carácter accesorio, se halle tan íntimamente ligada al secreto de lo comunicado que también merezca convertirse en objeto de protección constitucional. Como es sabido, la jurisprudencia constitucional, tomando como inspiración la STEDH de 2 agosto de 1982 – *Caso Malone* –, ha venido insistiendo en que la protección alcanza frente a cualquier forma de interceptación en el proceso de comunicación mientras el proceso está teniendo lugar, siempre que sea apta para desvelar, ya sea la existencia misma de la comunicación, el contenido de lo comunicado o los *elementos externos del proceso de comunicación* (cfr. SSTC 114/1984, de 29 de noviembre; 123/2002, de 20 de mayo; 137/2002, de 3 de junio; 281/2006, 9 de octubre. … Aceptado, pues, que nuestro régimen jurídico impone la exigencia de autorización judicial para la cesión por las operadoras del IMSI –también en los casos de telefonía móvil mediante tarjeta prepago-, hemos de cuestionarnos si el acceso a ese dato –no su cesión- puede obtenerse legítimamente por las Fuerzas y Cuerpos de Seguridad del Estado, sin necesidad de autorización judicial previa. La primera idea que sugiere la lectura de la Ley 25/2007 es que sus preceptos se centran en ofrecer un casuístico régimen jurídico de la conservación y cesión por las operadoras de los datos relativos a las comunicaciones electrónicas –en nuestro caso, del IMSI-, pero no aborda la regulación de su recogida por las Fuerzas y Cuerpos de Seguridad del Estado, no desde los ficheros automatizados que obran en poder de los prestadores de servicio, sino desde el propio teléfono celular. Cobra todo su significado el régimen jurídico del acceso a los ficheros contemplado por la LO 15/1999, 13 de diciembre, de protección de datos. Y es que frente al silencio de la nueva regulación, esta ley dispone que —la recogida y tratamiento para fines policiales de datos de carácter personal por las Fuerzas y Cuerpos de Seguridad sin consentimiento de las personas afectadas están limitados a aquellos supuestos y categorías de datos que resulten necesarios para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales, debiendo ser almacenados en ficheros específicos establecidos al efecto, que deberán clasificarse por categorías en función de su grado de fiabilidad (art. 22.2). Además, —la recogida y tratamiento por las Fuerzas y Cuerpos de Seguridad de los datos, a que hacen referencia los apartados 2 y 3 del artículo 7, podrán realizarse exclusivamente en los supuestos en que sea absolutamente necesario para los fines de una investigación concreta, sin perjuicio del control de legalidad de la actuación administrativa o de la obligación de resolver las pretensiones formuladas en su caso por los interesados que corresponden a los órganos

não proteção constitucional. Citando o célebre caso *Malone vs. The United Kingdom*[412], a Corte observou que haveria uma insistência para que a proteção constitucional alcançasse qualquer forma de interceptação sobre o processo comunicativo enquanto este estivesse ocorrendo, sempre que fosse apta a revelar a própria existência da comunicação ou seu conteúdo, mas também para que alcançasse os elementos externos do processo comunicativo. Considerando que a legislação espanhola exige autorização judicial prévia também para a cessão de dados de tráfego (no caso deste precedente, tratava-se da obtenção do número IMSI), a Corte vislumbrou a necessidade de se questionar se o mero acesso a tais dados (e não a cessão destes) também demandaria intervenção judicial. Entendeu-se que a Ley 25/2007, embora estabelecesse um regime jurídico para conservação e cessão dos dados relativos às comunicações eletrônicas pelas operadoras, não teria regulamentado a aquisição desses mesmos dados pelas forças de segurança do Estado.

Diante disso, a Corte voltou olhos para a legislação anterior (Ley 15/1999), tendo verificado que aquela dispôs sobre a possibilidade de o Estado acessar dados relativos a comunicações sem exigir ordem judicial prévia.

No entanto, entendeu o Tribunal que tal constatação não pode instituir um regime de ausência de controle em favor dos órgãos de persecução e, por outro lado, que a obtenção desses dados numa investigação criminal, mesmo que sem ordem judicial, pode perfeitamente ser reputada proporcional, necessária e não violadora da Constituição. Até porque –

---

jurisdiccionales‖ (art. 22.3). Esa capacidad de recogida de datos que la LO 15/1999, 13 de diciembre, otorga a las Fuerzas y Cuerpos de Seguridad del Estado, no puede, desde luego, servir de excusa para la creación de un régimen incontrolado de excepcionalidad a su favor. Pero tampoco cabe desconocer que la recogida de ese dato en el marco de una investigación criminal –nunca con carácter puramente exploratorio-, para el esclarecimiento de un delito de especial gravedad, puede reputarse proporcionada, necesaria y, por tanto, ajena a cualquier vulneración de relieve constitucional. También parece evidente que esa legitimidad que la ley confiere a las Fuerzas y Cuerpos de Seguridad del Estado nunca debería operar en relación con datos referidos al contenido del derecho al secreto de las comunicaciones (art. 18.3 de la CE) o respecto de datos susceptibles de protección por la vía del art. 18.4 de la CE que afectaran a lo que ha venido en llamarse el núcleo duro de la privacidad o, con la terminología legal, los datos especialmente protegidos (art. 7.2 LO 15/1999). Hecha la anterior precisión, está fuera de dudas que el IMSI, por sí solo, no es susceptible de ser incluido en alguna de esas dos categorías. Ni es un dato integrable en el concepto de comunicación, ni puede ser encuadrado entre los datos especialmente protegidos. Como ya se razonó *supra,* ese número de identificación sólo expresa una serie alfanumérica incapaz de identificar, por su simple lectura, el número comercial del abonado u otros datos de interés para la identificación de la llamada. Para que la numeración IMSI brinde a los investigadores toda la información que alberga, es preciso que esa serie numérica se ponga en relación con otros datos que obran en poder del operador. Y es entonces cuando las garantías propias del derecho a la autodeterminación informativa o, lo que es lo mismo, del derecho a controlar la información que sobre cada uno de nosotros obra en poder de terceros, adquieren pleno significado. Los mismos agentes de Policía que hayan logrado la captación del IMSI en el marco de la investigación criminal, habrán de solicitar autorización judicial para que la operadora correspondiente ceda en su favor otros datos que, debidamente tratados, permitirán obtener información singularmente valiosa para la investigación. En definitiva, así como la recogida o captación técnica del IMSI no necesita autorización judicial, sin embargo, la obtención de su plena funcionalidad, mediante la cesión de los datos que obran en los ficheros de la operadora, sí impondrá el control jurisdiccional de su procedencia."

[412] Ver item 3.2.2, sobre a influência do caso *Malone* sobre a legislação inglesa reguladora da medida de interceptação de comunicações.

prosseguiu a Corte –, esta possibilidade (decorrente da Ley 15/1999) que os órgãos de persecução têm de obter dados como o IMSI independentemente de ordem judicial nunca haverá de se operar sobre informações efetivamente atinentes ao sigilo das comunicações (o conteúdo comunicativo protegido pelo artigo 18.3 da Constituição espanhola) ou sobre o que chamou de "núcleo duro da privacidade" (segundo os termos da Ley 15/1999, são os dados especialmente protegidos[413]). E o IMSI, por si só, quando desacompanhado de outros dados, não se enquadraria em nenhuma das duas categorias, pois não seria capaz sequer de identificar o usuário. Por fim, restou decidido que fica dispensada de autorização judicial a obtenção do IMSI pelos órgãos de persecução, o que não ocorrerá quando se estiver diante de cessão de dados de tráfego em sua plena funcionalidade, visto que tal cessão, esta sim reveladora de informações atinentes ao sigilo das comunicações, deverá ser precedida de intervenção judicial.

Mais recentemente, em 2010, a *Sala de lo Penal* do *Tribunal Supremo* ratificou este entendimento ao julgar questão semelhante. Disse que não há necessidade de prévia autorização judicial para o acesso ao código IMEI, tendo em vista que este não contém o número telefônico do investigado, dado que só poderia ser obtido mediante cessão de dados pela operadora, tendo a Corte feito observar, ainda, que tal matéria já seria pacífica naquele colegiado[414].

Pode-se notar, portanto, o nível de controvérsia existente em torno da questão, tanto da inserção do direito ao sigilo dos dados relativos a comunicações no âmbito de proteção do direito constitucional ao sigilo das comunicações, quanto da necessidade de ordem judicial para o acesso a tais dados por parte de órgãos de persecução.

Apesar das divergências, vale observar o método adotado pelo *Tribunal Supremo*, em 2009, de distinção entre dados atinentes e não atinentes ao sigilo das comunicações. Pode-se

---

[413] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. "Artículo 7. Datos especialmente protegidos. 2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado" (Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-1999-23750>. Acesso em: 30 mai. 2013).

[414] ESPANHA. Tribunal Supremo. Sala de lo Penal. STS 5606/2010, Recurso Casación nº 621/2010. Resolución 895/2010. 28079120012010100841. Disponível em: <http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=TS&reference=5781704&links=&optimize=20101118&publicinterface=true>. Acesso em: 29 mai. 2013: "Por ello, el código IMEI no contiene el número telefónico del abonado, que solo puede ser conocido si se le solicita a la operadora la cesión de esos datos. Por eso, la doctrina de esta Sala, de manera clara – con alguna sentencia aislada, como la 130/2007 de 19 de Febrero – tiene declarado que la captura de esse número IMEI no forma parte de la cobertura que otorga el art. 18-3º C.E. – Dicho más claramente la captura del IMEI no precisa autorización judicial."

dizer que, no caso STS 1550/2010, a Corte apresentou uma espécie de sistematização acerca do tema. De início, observou a existência de uma súmula editada por sua *Sala General no jurisdicional* dispondo que o órgão de acusação precisará obter ordem judicial para ter direito a requisitar das operadoras de comunicação os dados relativos a comunicações, mais precisamente aqueles elencados no artigo 3º da Ley 25/2007. No entanto, invocou o caso Malone[415] e dele extraiu a afirmação de que a proteção ao sigilo de comunicações alcançaria qualquer forma de interceptação em processo de comunicação enquanto este esteja ocorrendo, sempre que tal interceptação seja apta a revelar a existência da própria comunicação, seu conteúdo ou elementos externos do processo comunicativo.

Prosseguiu a Corte sustentando que a interpretação correta de tal entendimento deve levar à distinção entre dados pessoais que possam afetar o sigilo das comunicações daqueles que, embora conservados por operadoras de comunicações, sejam estaticamente armazenados, mas não se refiram a comunicação alguma. Nesse sentido, concebeu dois conceitos:

a) dados pessoais externos ou de tráfego que façam referência a uma comunicação concreta e contribuem para revelar todo ou parte do segredo protegido pelo artigo 18.3 da Constituição espanhola; e
b) dados ou circunstâncias pessoais referentes à intimidade de uma pessoa, mas que sejam autônomos ou desconectados de qualquer comunicação, estando estes protegidos pelo direito à proteção de dados informáticos ou *habeas data* assegurados no artigo 18.4 da Constituição.

Por fim, a Corte concluiu, a partir dessa perspectiva dicotômica, que os dados relativos a comunicações concretamente realizadas é que são aqueles compreendidos no âmbito de proteção do artigo 18.3, pois a inclusão absoluta de todo tipo de dados de tráfego ou externos sob a mesma proteção acabaria por igualar circunstâncias cujo tratamento jurídico deveria ser distinto[416].

---

[415] Sobre o caso Malone vs. The United Kingdom, ver item 3.2.2.

[416] ESPANHA. Tribunal Supremo. Sala de lo Penal. STS 1550/2010. Recurso casación nº 121/2009. Resolución 247/2010. 28079120012010100231. Disponível em: <http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=TS&reference=5554451&links=informaticos&optimize=20100422&publicinterface=true>. Acesso em: 29 mai. 2013: "La Sala General no jurisdiccional aprobó el 23 de febrero de 2010 el siguiente acuerdo: 'Es necesaria la autorización judicial para que los operadores que prestan servicios de comunicaciones electrónicas o de redes públicas de comunicación cedan los datos generados o tratados con tal motivo. Por lo cual, el Mº Fiscal precisará de tal autorización para obtener de los operadores los datos conservados que se especifican en el art. 3 de la Ley 25/2007 de 18 de octubre'. De conformidad al tenor del acuerdo es patente que no resulta de aplicación al caso que nos concierne por haber ocurrido los hechos en 2006, esto es, antes de su vigencia. 3. Acudiendo a las normas en vigor que

A Ley 25/2007 trata especificamente dos dados de tráfego e da importância de sua conservação para fins investigativos, anunciando, já no artigo 1º, que a lei tem por objeto regular a obrigação de conservar dados decorrentes da prestação de serviços de comunicações eletrônicas e de ceder esses dados, mediante autorização judicial, para fins de investigação, prisão e processo por delitos graves previstos no Código Penal ou em leis penais especiais. Tal fornecimento é restrito às forças de segurança que desempenhem funções de polícia judiciária, à *Dirección Adjunta de Vigilancia Aduanera* e ao *Centro Nacional de Inteligencia*[417].

---

garantizan la reserva de las claves encubridoras de la identidad de usuarios de la Red (I.P.), se hace preciso de nuevo recordar la doctrina del Tribunal de Derechos Humanos europeo (caso Malone), contenido en la sentencia de 2 de agosto de 1982, que viene a establecer que la protección del derecho al secreto de las comunicaciones alcanza "a cualquier forma de interceptación em el proceso de comunicación, mientras el mismo esté teniendo lugar, siempre que sea apta para desvelar la existencia misma de la comunicación, el contenido de lo comunicado o los datos o elementos externos del proceso de comunicación". La correcta interpretación de esta doctrina nos debe llevar a la distinción de cuándo unos datos personales pueden afectar al secreto a las comunicaciones y cuándo conservados y tratados por las Operadoras, no se están refiriendo a comunicación alguna, es decir, datos estáticamente almacenados, conservados y tratados por operadores que se hallan obligados a la reserva frente a terceros. Distinguimos pues dos conceptos: a) datos personales externos o de tráfico que hacen referencia a una comunicación concreta y contribuyen a desvelar todo o parte del secreto que protege el art. 18-3 C.E; b) datos o circunstancias personales referentes a la intimidad de una persona (art. 18-1º C.E.), pero *autónomos o desconectados* de cualquier comunicación, que caerán dentro del derecho a la protección de datos informáticos o *habeas data* del art. 18-4 C.E. que no pueden comprometer un proceso de comunicación. Desde esta perspectiva dicotómica la absoluta equiparación de todo tipo de datos de tráfico o externos o la inclusión de todos ellos dentro del derecho al secreto de las comunicaciones comportaría un auténtico desenfoque del problema, pues incorporaría en el ámbito de la protección constitucional del art. 18-3, circunstancias cuyo tratamiento jurídico no debería separarse del que se dispensa a la protección de datos o al derecho a la autodeterminación informática del art. 18-4 C.E. (véase por todas S.T.S. nº 249 de 20-5-2008). 4. En el caso concernido es patente que los datos cuyo obtención se pretende por el Fiscal no tienen relación ni afecan ni interceptan ni descubren ni tratan de descubrir una comunicación concreta, sino que por ser preciso para la acción investigadora el conocimiento del domicilio, número de teléfono o identidad del titular del terminal informático que opera en la Red (I.P.), la solicita a la operadora, al objeto de pedir del juez um mandameinto de entrada y registro con fines indagatorios o de investigación de un posible delito, acerca del que se conocen datos indiciarios."

[417] Ley 25/2007. "Artículo 1. Objeto de la Ley. 1. Esta Ley tiene por objeto la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales. 2. Esta Ley se aplicará a los datos de tráfico y de localización sobre personas físicas y jurídicas y a los datos relacionados necesarios para identificar al abonado o usuario registrado. ... Artículo 6. Normas generales sobre cesión de datos. 1. Los datos conservados de conformidad con lo dispuesto en esta Ley sólo podrán ser cedidos de acuerdo con lo dispuesto en ella para los fines que se determinan y previa autorización judicial. 2. La cesión de la información se efectuará únicamente a los agentes facultados. A estos efectos, tendrán la consideración de agentes facultados: a) Los miembros de las Fuerzas y Cuerpos de Seguridad, cuando desempeñen funciones de policía judicial, de acuerdo con lo previsto en el artículo 547 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial. b) Los funcionarios de la Dirección Adjunta de Vigilancia Aduanera, en el desarrollo de sus competencias como policía judicial, de acuerdo con el apartado 1 del artículo 283 de la Ley de Enjuiciamiento Criminal. c) El personal del Centro Nacional de Inteligencia en el curso de las investigaciones de seguridad sobre personas o entidades, de acuerdo con lo previsto en la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, y en la Ley Orgánica 2/2002, de 6 de mayo, reguladora del control judicial previo del Centro Nacional de Inteligencia". (Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-2007-18243>. Acesso em 03 de abr. 2013).

A lei distingue, expressamente, o regime de tratamento legal do acesso a esses dados de tráfego de conservação obrigatória e ao conteúdo de comunicações, ao dispor que "*se excluye del ámbito de aplicación de esta Ley el contenido de las comunicaciones electrónicas*"[418].

Embora em 2003, com a *Ley General de Telecomunicaciones*, já houvesse uma lista de dados de tráfego a serem armazenados pelos prestadores de serviços de comunicações[419], foi o artigo 3º da Ley 25/2007 que tratou mais profundamente da matéria, dispondo que deverão ser armazenados telefone, endereço, identificação e IP do assinante e de qualquer interlocutor que com ele se comunique; data, hora e duração das comunicações; data e hora da conexão e desconexão do acesso à internet, baseadas num determinado fuso horário, o endereço vinculado ao IP, seja ele dinâmico ou estático[420], a data e hora de conexão e

---

[418] Ley 25/2005. "Artículo 1. Objeto de la Ley. ... 3. Se excluye del ámbito de aplicación de esta Ley el contenido de las comunicaciones electrónicas, incluida la información consultada utilizando una red de comunicaciones electrónicas. ... Artículo 3. Datos objeto de conservación. … 2. Ningún dato que revele el contenido de la comunicación podrá conservarse en virtud de esta Ley" (Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-2007-18243>. Acesso em: 28 mai. 2013).

[419] Ley 32/2003. "Artículo 33. Secreto de las comunicaciones. … 5. Los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición y sin perjuicio de otros datos que puedan ser establecidos mediante real decreto, los datos indicados en la orden de interceptación legal, de entre los que se relacionan a continuación: a) Identidad o identidades del sujeto objeto de la medida de la interceptación. Se entiende por identidad: etiqueta técnica que puede representar el origen o el destino de cualquier tráfico de comunicaciones electrónicas, en general identificada mediante un número de identidad de comunicaciones electrónicas físico (tal como un número de teléfono) o un código de identidad de comunicaciones electrónicas lógico o virtual (tal como un número personal) que el abonado puede asignar a un acceso físico caso a caso. b) Identidad o identidades de las otras partes involucradas en la comunicación electrónica. c) Servicios básicos utilizados. d) Servicios suplementarios utilizados. e) Dirección de la comunicación. f) Indicación de respuesta. g) Causa de finalización. h) Marcas temporales. i) Información de localización. j) Información intercambiada a través del canal de control o señalización. 6. Además de la información relativa a la interceptación prevista en el apartado anterior, los sujetos obligados deberán facilitar al agente facultado, salvo que por las características del servicio no estén a su disposición y sin perjuicio de otros datos que puedan ser establecidos mediante real decreto, de cualquiera de las partes que intervengan en la comunicación que sean clientes del sujeto obligado, los siguientes datos: a) Identificación de la persona física o jurídica. b) Domicilio en el que el proveedor realiza las notificaciones. Y, aunque no sea abonado, si el servicio de que se trata permite disponer de alguno de los siguientes: c) Número de titular de servicio (tanto el número de directorio como todas las identificaciones de comunicaciones electrónicas del abonado). d) Número de identificación del terminal. e) Número de cuenta asignada por el proveedor de servicios internet. f) Dirección de correo electrónico. 7. Junto con los datos previstos en los apartados anteriores, los sujetos obligados deberán facilitar, salvo que por las características del servicio no esté a su disposición, información de la situación geográfica del terminal o punto de terminación de red origen de la llamada, y de la del destino de la llamada. En caso de servicios móviles, se proporcionará una posición lo más exacta posible del punto de comunicación y, en todo caso, la identificación, localización y tipo de la estación base afectada. 8. Con carácter previo a la ejecución de la orden de interceptación legal, los sujetos obligados deberán facilitar al agente facultado información sobre los servicios y características del sistema de telecomunicación que utilizan los sujetos objeto de la medida de la interceptación y, si obran en su poder, los correspondientes nombres de los abonados con sus números de documento nacional de identidad, tarjeta de residencia o pasaporte, en el caso de personas físicas, o denominación y código de identificación fiscal en el caso de personas jurídicas" (Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-2003-20253>. Acesso em: 25 mai 2013).

[420] O IP pode ser fixo para um determinado usuário (IP estático) ou variável ao longo do período em que esse usuário permanece conectado (IP dinâmico). A diferenciação se mostrará relevante porque gerará mudança no regime de proteção a tal dado. "Esta IP puede ser estática, en cuyo caso se asemeja al número de telefono, dato previo a la conexión del terminal e invariavle en cada conexión, encajando en la categoria emplia de datos de

desconexão do serviço de correio eletrônico e a identificação dos equipamentos e aparelhos utilizados na comunicação[421].

O prazo durante o qual deve perdurar o armazenamento de dados é de doze meses, podendo ser alterado para um máximo de dois anos e um mínimo de seis meses, para o que se deverá levar em conta, de um lado, o custo do armazenamento e, de outro, o interesse público para fins de investigação, detenção e instauração de processo por um crime grave[422].

---

suscripción, o dinâmica, que puede cambiar en cada conexión e incluso durante ésta. La IP dinâmica, al igual que el momento y duración de la conexión, son datos cinculados a la concreta conexión en el marco de la cual se efectúan (o no) distintas comunicaciones" (LÓPEZ, 2012, p. 123).

[421] Ley 25/2007. "Artículo 3. Datos objeto de conservación. 1. Los datos que deben conservarse por los operadores especificados en el artículo 2 de esta Ley, son los siguientes: a) Datos necesarios para rastrear e identificar el origen de una comunicación: 1.° Con respecto a la telefonía de red fija y a la telefonía móvil: i) Número de teléfono de llamada. ii) Nombre y dirección del abonado o usuario registrado. 2.° Con respecto al acceso a internet, correo electrónico por internet y telefonía por internet: i) La identificación de usuario asignada. ii) La identificación de usuario y el número de teléfono asignados a toda comunicación que acceda a la red pública de telefonía. iii) El nombre y dirección del abonado o del usuario registrado al que se le ha asignado en el momento de la comunicación una dirección de Protocolo de Internet (IP), una identificación de usuario o un número de teléfono. b) Datos necesarios para identificar el destino de una comunicación: 1.º Con respecto a la telefonía de red fija y a la telefonía móvil: i) El número o números marcados (el número o números de teléfono de destino) y, en aquellos casos en que intervengan otros servicios, como el desvío o la transferencia de llamadas, el número o números hacia los que se transfieren las llamadas. ii) Los nombres y las direcciones de los abonados o usuarios registrados. 2.º Con respecto al correo electrónico por internet y la telefonía por internet: i) La identificación de usuario o el número de teléfono del destinatario o de los destinatarios de una llamada telefónica por internet. ii) Los nombres y direcciones de los abonados o usuarios registrados y la identificación de usuario del destinatario de la comunicación. c) Datos necesarios para determinar la fecha, hora y duración de una comunicación: 1.° Con respecto a la telefonía de red fija y a la telefonía móvil: la fecha y hora del comienzo y fin de la llamada o, en su caso, del servicio de mensajería o del servicio multimedia. 2.° Con respecto al acceso a internet, al correo electrónico por internet y a la telefonía por internet: i) La fecha y hora de la conexión y desconexión del servicio de acceso a internet registradas, basadas en un determinado huso horario, así como la dirección del Protocolo Internet, ya sea dinámica o estática, asignada por el proveedor de acceso a internet a una comunicación, y la identificación de usuario o del abonado o del usuario registrado. ii) La fecha y hora de la conexión y desconexión del servicio de correo electrónico por internet o del servicio de telefonía por internet, basadas en un determinado huso horario. d) Datos necesarios para identificar el tipo de comunicación. 1.° Con respecto a la telefonía de red fija y a la telefonía móvil: el servicio telefónico utilizado: tipo de llamada (transmisión de voz, buzón vocal, conferencia, datos), servicios suplementarios (incluido el reenvío o transferencia de llamadas) o servicios de mensajería o multimedia empleados (incluidos los servicios de mensajes cortos, servicios multimedia avanzados y servicios multimedia). 2.° Con respecto al correo electrónico por internet y a la telefonía por internet: el servicio de internet utilizado. e) Datos necesarios para identificar el equipo de comunicación de los usuarios o lo que se considera ser el equipo de comunicación: 1.º Con respecto a la telefonía de red fija: los números de teléfono de origen y de destino. 2.° Con respecto a la telefonía móvil: i) Los números de teléfono de origen y destino. ii) La identidad internacional del abonado móvil (IMSI) de la parte que efectúa la llamada. iii) La identidad internacional del equipo móvil (IMEI) de la parte que efectúa la llamada. iv) La IMSI de la parte que recibe la llamada. v) La IMEI de la parte que recibe la llamada. vi) En el caso de los servicios anónimos de pago por adelantado, tales como los servicios con tarjetas prepago, fecha y hora de la primera activación del servicio y la etiqueta de localización (el identificador de celda) desde la que se haya activado el servicio. 3.° Con respecto al acceso a internet, correo electrónico por internet y telefonía por internet: i) El número de teléfono de origen en caso de acceso mediante marcado de números. ii) La línea digital de abonado (DSL) u otro punto terminal identificador del autor de la comunicación. f) Datos necesarios para identificar la localización del equipo de comunicación móvil: 1.° La etiqueta de localización (identificador de celda) al inicio de la comunicación. 2.° Los datos que permiten fijar la localización geográfica de la celda, mediante referencia a la etiqueta de localización, durante el período en el que se conservan los datos de las comunicaciones" (Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-2007-18243>. Acesso em: 25 mai. 2013).

[422] Ley 25/2007. "Artículo 5. Período de conservación de los datos. 1. La obligación de conservación de datos impuesta cesa a los doce meses computados desde la fecha en que se haya producido la comunicación.

O artigo 8.1 da Ley 25/2007 demonstra a preocupação do legislador em impedir a manipulação, destruição acidental ou ilícita ou, ainda, perda acidental dos dados de tráfego armazenados, impondo a adoção de medidas técnicas para tanto[423].

O mesmo diploma, inclusive, instituiu uma exceção ao chamado direito ao cancelamento, que, por força de lei diversa[424], dá ao cidadão a possibilidade de exigir a supressão das informações que existirem a seu respeito em bancos de dados públicos ou privados[425]. Por força de tal exceção legal, o prestador de serviços de comunicações terá que denegar eventual pedido de exercício deste direito, se o cliente usuário o formular.

3.3.4 Regulamentação da criptografia

A *Ley General de Telecomunicaciones* (32/2003), em seu artigo 36, autoriza expressamente o uso de criptografia, que define como um instrumento de segurança da informação, mas estabelece, entre suas condições de uso, a prerrogativa do Estado de impor a obrigação de facilitar a um órgão estatal os meios e equipamentos, sem custo algum, para descriptografar[426].

Reglamentariamente, previa consulta a los operadores, se podrá ampliar o reducir el plazo de conservación para determinados datos o una categoría de datos hasta un máximo de dos años o un mínimo de seis meses, tomando en consideración el coste del almacenamiento y conservación de los datos, así como el interés de los mismos para los fines de investigación, detección y enjuiciamiento de un delito grave, previa consulta a los operadores" (Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-2007-18243>. Acesso em: 25 mai. 2013).

[423] Ley 25/2007. "Artículo 8. Protección y seguridad de los datos. 1. Los sujetos obligados deberán identificar al personal especialmente autorizado para acceder a los datos objeto de esta Ley, adoptar las medidas técnicas y organizativas que impidan su manipulación o uso para fines distintos de los comprendidos en la misma, su destrucción accidental o ilícita y su pérdida accidental, así como su almacenamiento, tratamiento, divulgación o acceso no autorizados, con sujeción a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, y en su normativa de desarrollo". (Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-2007-18243>. Acesso em: 27 mai. 2013).

[424] O *derecho de rectificación y cancelación* está previso no artigo 16 da Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal ((Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-1999-23750>. Acesso em: 27 mai. 2013).

[425] Ley 25/2007. "Artículo 9. Excepciones a los derechos de acceso y cancelación. 1. El responsable del tratamiento de los datos no comunicará la cesión de datos efectuada de conformidad con esta Ley. 2. El responsable del tratamiento de los datos denegará el ejercicio del derecho de cancelación en los términos y condiciones previstos en la Ley Orgánica 15/1999, de 13 de diciembre" (Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-2007-18243>. Acesso em: 28 mai. 2013).

[426] Ley 32/2003. "Artículo 36. Cifrado en las redes y servicios de comunicaciones electrónicas. 1. Cualquier tipo de información que se transmita por redes de comunicaciones electrónicas podrá ser protegida mediante procedimientos de cifrado. 2. El cifrado es un instrumento de seguridad de la información. Entre sus condiciones de uso, cuando se utilice para proteger la confidencialidad de la información, se podrá imponer la obligación de facilitar a un órgano de la Administración General del Estado o a un organismo público, los algoritmos o cualquier procedimiento de cifrado utilizado, así como la obligación de facilitar sin coste alguno los aparatos de

No caso de tecnologias de comunicações cujo processo comunicativo já se dê naturalmente por meio de compressão, cifragem, digitalização ou qualquer outro tipo de codificação, o artigo 33 da mesma *Ley* 32/2003[427] e o artigo 96 do *Real Decreto* 424/2005[428], de teor semelhante, também impõem aos prestadores de serviços de comunicações o dever de fornecer ao órgão investigador as comunicações desprovidas dos efeitos de tais procedimentos, sempre que sejam reversíveis, impondo-lhes, ainda, o dever de fornecer as comunicações interceptadas com uma qualidade não inferior à que o destinatário obtém.

3.3.5 Inutilização de material interceptado

A Ley Orgánica 2/2002, em seu artigo único, inciso 4, dispõe que o Secretário de Estado Diretor do Centro Nacional de Inteligência ordenará "*la inmediata destrucción del material relativo a todas aquellas informaciones que, obtenidas mediante la autorización prevista en este artículo, no guarden relación con el objeto o fines de la misma*"[429].

A prerrogativa abre possibilidade de supressão de material probatório sem que haja, na lei, dispositivo voltado para assegurar a fiscalização da medida ou a participação da defesa. A legislação brasileira, ao contrário, traz dispositivo contendo tal preocupação, embora com redação que dá margens a interpretações inadequadas sobre o direito da defesa de acompanhar eventual destruição de material digital captado em interceptações. A questão será enfrentada no item 4.7.

---

cifra a efectos de su control de acuerdo con la normativa vigente" (Disponível em: <http://www.boe.es/buscar/doc.php?id=BOE-A-2003-20253>. Acesso em: 28 mai. 2013).

[427] Ley 32/2003. "Artículo 33 ... 10. En el caso de que los sujetos obligados apliquen a las comunicaciones objeto de interceptación legal algún procedimiento de compresión, cifrado, digitalización o cualquier otro tipo de codificación, deberán entregar aquellas desprovistas de los efectos de tales procedimientos, siempre que sean reversibles. Las comunicaciones interceptadas deben proveerse al centro de recepción de las interceptaciones con una calidad no inferior a la que obtiene el destinatario de la comunicación" (Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-2003-20253>. Acesso em: 28 mai. 2013).

[428] Real Decreto 424/2005. Artículo 96. Señal en claro y calidad de la señal entregada. En el caso de que los sujetos obligados apliquen a las comunicaciones objeto de interceptación legal algún procedimiento de compresión, cifrado, digitalización o cualquier otro tipo de codificación, deberán entregar aquellas desprovistas de los efectos de tales procedimientos, siempre que sean reversibles. Las comunicaciones interceptadas deben proveerse al centro de recepción de las interceptaciones con una calidad no inferior a la que obtiene el destinatario de la comunicación. (Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-2005-6970>. Acesso em: 25 mai. 2013).

[429] Ley orgânica 2/2002. "Artículo único. Control judicial previo del Centro Nacional de Inteligencia. ... 4. El Secretario de Estado Director del Centro Nacional de Inteligencia ordenará la inmediata destrucción del material relativo a todas aquellas informaciones que, obtenidas mediante la autorización prevista en este artículo, no guarden relación con el objeto o fines de la misma" (Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-2002-8627>. Acesso em: 28 mai. 2013).

3.3.6 Sanções penais e administrativas para interceptação e divulgação ilegais do produto de interceptação e para o descumprimento do dever de facilitar interceptação e de armazenar dados relativos a comunicações eletrônicas

O Código Penal espanhol, no título "*Delitos contra la intimidad, el derecho a la propia imagen y la inviolabilidad del domicilio*", mais precisamente no capítulo "*Del descubrimiento y revelación de secretos*", comina pena de prisão de um a quatro anos e multa para aquele que, para vulnerar a intimidade de alguém ou descobrir seus segredos, sem seu consentimento, se apodera de papéis, cartas, mensagens de correio eletrônico ou quaisquer outros documentos ou intercepta suas telecomunicações ou utiliza artifícios técnicos de escuta, transmissão, gravação ou reprodução do som ou da imagem ou qualquer outro sinal de comunicação[430].

Já a divulgação do material sigiloso acessado ilegalmente é punida com pena de dois a cinco anos de prisão ou, para o agente que não tiver tomado parte na conduta de acessar ilegalmente, um a três anos[431].

Se o crime for cometido com fins de lucro ou se o material sigiloso for relativo a informações pessoais ligadas a ideologia, religião, crença, saúde, origem racial, vida sexual ou se a vítima for menor ou incapaz, a pena será aplicada acima da metade entre a mínima e a máxima previstas. Se houver finalidade de obtenção de lucro concomitante à condição relativa ao conteúdo do material, a pena será de quatro a sete anos[432].

---

[430] Ley Orgánica 10/1995 (Código Penal). "Artículo 197. 1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses" (Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-1995-25444>. Acesso em: 06 mai. 2013).

[431] Ley Orgánica 10/1995 (Código Penal). "Artículo 197. … 4. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores. Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior" (Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-1995-25444>. Acesso em: 28 mai. 2013).

[432] Ley Orgánica 10/1995 (Código Penal). "Artículo 197. … 6. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior. 7. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado anterior, la pena a imponer será la de prisión de cuatro a siete años" (Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-1995-25444>. Acesso em: 17 mai. 2013).

Se a violação da intimidade ou do sigilo for praticada por quem tenha o dever de zelar por eles, a exemplo dos operadores de serviços de comunicações, a pena será de três a cinco anos, devendo esta ser fixada acima da metade entre a mínima e a máxima no caso de o agente também divulgar o material sigiloso[433].

As mesmas penas se aplicam a violações de dados reservados pertencentes a pessoas jurídicas sem consentimento de seus representantes[434].

No campo administrativo, definiram-se como infrações muito graves as condutas de interceptar comunicações sem autorização; divulgar o conteúdo ou a simples existência de mensagens privadas captadas por interceptação voluntária ou involuntária; o descumprimento e o atraso no cumprimento por parte de operadores de serviços de comunicações das obrigações de facilitar as interceptações legalmente autorizadas; e o descumprimento do dever de armazenar dados de comunicações eletrônicas tal qual previsto na chamada *Ley de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones* (25/2007). Para tais condutas, estabeleceu-se sanção de inabilitação do operador de serviço de comunicações por até cinco anos, além de multa em valor não superior ao quíntuplo da vantagem que o agente auferiu ou, em casos em que não seja possível apurar vantagem financeira, limitada a dois milhões de euros[435].

---

[433] Ley Orgánica 10/1995 (Código Penal). "Artículo 197. …5. Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior" (Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-1995-25444>. Acesso em: 14 mai. 2013).

[434] Ley Orgánica 10/1995 (Código Penal). "Artículo 200. Lo dispuesto en este capítulo será aplicable al que descubriere, revelare o cediere datos reservados de personas jurídicas, sin el consentimiento de sus representantes, salvo lo dispuesto en otros preceptos de este Código" (Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-1995-25444>. Acesso em: 21 mai. 2013).

[435] Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones. "Artículo 53. Infracciones muy graves. Se consideran infracciones muy graves: … n) La interceptación, sin autorización, de telecomunicaciones no destinadas al público en general. ñ) La divulgación del contenido, o de la simple existencia, de mensajes no destinados al público en general emitidos o recibidos a través de servicios de telecomunicaciones, a los que se acceda mediante la interceptación voluntaria o involuntaria, su publicación o cualquier otro uso de ellos sin la debida autorización. o) El incumplimiento deliberado, por parte de los operadores, de las obligaciones en materia de interceptación legal de comunicaciones impuestas en desarrollo del artículo 33 de esta Ley y el incumplimiento deliberado de las obligaciones de conservación de los datos establecidas en la Ley de Conservación de Datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones. … Artículo 56. Sanciones. 1. El Ministerio de Ciencia y Tecnología o la Comisión del Mercado de las Telecomunicaciones impondrán, en el ámbito de sus respectivas competencias, las siguientes sanciones: … b) Por la comisión de las demás infracciones muy graves se impondrá al infractor multa por importe no inferior al tanto, ni superior al quíntuplo, del beneficio bruto obtenido como consecuencia de los actos u omisiones en que consista la infracción. En caso de que no resulte posible aplicar este criterio, el límite máximo de la sanción será de dos millones de euros. Las infracciones muy graves, en función de sus circunstancias, podrán dar lugar a la inhabilitación hasta de cinco años del operador para la explotación de redes o la prestación de servicios de comunicaciones electrónicas" (Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-2003-20253>. Acesso em: 28 mai. 2013). Real Decreto 424/2005. "Artículo 101. Infracciones. 1. Sin perjuicio de la responsabilidad penal en que pueda incurrirse en la ejecución de las interceptaciones, el incumplimiento de las órdenes de interceptación legal será constitutivo de una infracción sancionable de acuerdo con las previsiones del

3.3.7 Aspectos mais relevantes

A Constituição espanhola assegura o direito à intimidade pessoal e familiar e o segredo das comunicações, em especial, as postais, telegráficas e telefônicas, exceto diante de decisão judicial. A doutrina, no entanto, estende o rol constitucional às chamadas comunicações eletrônicas.

A doutrina espanhola construiu os conceitos de comunicação em *canal abierto* e comunicação em *canal cerrado*, a primeira podendo ser exemplificada por páginas da *web* de livre acesso, fóruns, *chats* ou grupos de notícias não restritos e servidores FTP, e a última por e-mail, mensagens instantâneas ou qualquer outra forma de comunicação, incluídas aquelas que tenham seu funcionamento típico de *canal abierto* mas que operem com restrição do acesso dos participantes. Somente as comunicações em *canal cerrado* estão protegidas pelo direito ao sigilo das comunicações.

As comunicações eletrônicas poderão ser interceptadas por ordem judicial para descobrir ou comprovar algum fato ou circunstância importante da causa, ou caso a medida seja promovida sobre as comunicações de pessoa contra a qual haja indícios de responsabilidade criminal.

O prazo para a medida é de três meses, mas há permissão de prorrogações sem que haja limite legalmente estabelecido.

Apesar da exigência de ordem judicial, a *Ley de Enjuiciamiento Criminal* permite que, quando houver urgência, o Ministro do Interior ou, na falta deste, o Diretor de Segurança do Estado autorize interceptação de quadrilhas armadas e elementos terroristas. Nessas hipóteses, o juiz deverá ser avisado *a posteriori*, para decidir se irá manter ou revogar a medida.

Consta dispositivo legal impondo a adoção de todos os meios necessários para impedir a manipulação dos mecanismos de interceptação e para garantir a autenticidade, confidencialidade e integridade da informação obtida com a interceptação, o que demonstra diferenciada preocupação do legislador espanhol com a preservação da prova.

O prestador de serviço de comunicações incumbido de viabilizar a interceptação deverá notificar o agente investigador do momento em que o mecanismo de interceptação

---

título VIII de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones. 2. En la imposición de la sanción se valorará el retraso en la ejecución de la interceptación y otros perjuicios causados por el incumplimiento" (Disponível em: <http://www.boe.es/buscar/act.php?id=BOE-A-2005-6970>. Acesso em: 17 mai. 2013).

houver sido ativado, o que, a nosso ver, constitui um eficiente método de documentar o efetivo início da medida restritiva do direito fundamental.

A agência de inteligência espanhola, chamada de *Centro Nacional de Inteligencia*, poderá também pedir autorização judicial ao *Tribunal Supremo* para promover interceptação de comunicações, que, neste caso, será limitada a três meses, prorrogávis por igual período, em caso de necessidade. Nessa hipótese, no entanto, a medida não terá finalidade processual penal, mas sim a de obter e avaliar informações para proteger os interesses políticos, nacionais, econômicos, industriais, comerciais e estratégicos da Espanha.

Sobre a proteção a ser destinada aos dados de tráfego de comunicações na Espanha e sua inclusão ou exclusão no âmbito normativo do direito ao sigilo das comunicações, a jurisprudência passou por expressivas oscilações desde 1984, não estando consolidada até a atualidade.

Nesse sentido, em 1984, o *Tribunal Constitucional* afirmou que o artigo 18.3 da Constituição não cobre somente o conteúdo da comunicação, mas também outros aspectos, como a identidade dos interlocutores.

Em 2002, a mesma Corte decidiu que dados reveladores do telefone de destino, hora e duração da comunicação dependem de uma interferência no processo de comunicação e que, por isso, estariam compreendidos no âmbito do direito ao sigilo das comunicações, porém protegidos em menor intensidade do que o conteúdo das comunicações.

Em 2006, a Corte restringiu o âmbito de proteção do artigo 18.3 a somente o que constituísse conteúdo humano de comunicações.

Em 2007, voltou a afirmar que a identidade subjetiva dos interlocutores estaria abarcada pelo âmbito de proteção do artigo 18.3, dependendo o acesso a estes de ordem judicial.

Em 2008, o *Tribunal Supremo* decidiu que ficava dispensada autorização judicial para a obtenção de IMSI pelos órgãos de persecução, vindo a ratificar o mesmo entendimento em 2010 com relação à obtenção de IMEI.

Entre os dois julgados acima, em 2009, o *Tribunal Supremo* trouxe interessante raciocínio para distinguir aqueles dados externos ao processo comunicativo que estão protegidos daqueles que não estão protegidos pelo direito ao sigilo de comunicações. Entendeu o Tribunal por incluir no âmbito de proteção todo e qualquer dado que estivesse vinculado a uma comunicação concretamente realizada, excluindo todos os demais dados de tráfego.

A lei espanhola estabeleceu, também, o armazenamento obrigatório de determinados dados de tráfego pelos prestadores de serviços de comunicações, a saber, o telefone, endereço, identificação e IP do assinante e de qualquer interlocutor que com ele se comunique; a data, hora e duração das comunicações; a data e hora da conexão e desconexão do acesso à internet, baseadas num determinado fuso horário, o endereço vinculado ao IP, seja ele dinâmico ou estático, a data e a hora de conexão e desconexão do serviço de correio eletrônico e a identificação dos equipamentos e aparelhos utilizados na comunicação. Tal armazenamento deverá perdurar por doze meses, podendo ser alterado para um máximo de dois anos e um mínimo de seis meses, dependendo de critérios como o custo do armazenamento que o prestador de serviços terá e, de outro lado, o interesse público no acesso estatal àqueles dados para fins de investigação, detenção e instauração de processo por um crime grave.

A lei regulamenta o uso de criptografia, mas estabelece, entre suas condições de uso, a prerrogativa do Estado de impor a obrigação de facilitar a um órgão estatal os meios e equipamentos para descriptografar.

4 A INTERCEPTAÇÃO DAS COMUNICAÇÕES TELEMÁTICAS NO BRASIL

No Brasil, a proteção à intimidade e à privacidade é encontrada, embora não de forma direta ou expressa, desde a Constituição do Império, de 1824, na forma de inviolabilidade da casa e do segredo das cartas[436].

Nas Constituições posteriores, aí incluídas as de 1891[437], 1934[438], 1937[439] e 1946[440], com pequenas variações, mantiveram-se dispositivos protetores do sigilo da correspondência e da inviolabilidade do domicílio.

A Constituição de 1967 foi a primeira em que, junto à proteção à inviolabilidade da correspondência, foi assegurado o sigilo das comunicações telegráficas e telefônicas[441], o que se manteve com redação praticamente inalterada após a Emenda Constitucional nº 01 de 1969[442].

Mas foi somente na Constituição de 1988 que a inviolabilidade da intimidade e da vida privada foi expressamente prevista, no inciso X do artigo 5º.

---

[436] 1824: Art. 179 ... VII. Todo o Cidadão tem em sua casa um asylo inviolavel. De noite não se poderá entrar nella, senão por seu consentimento, ou para o defender de incendio, ou inundação; e de dia só será franqueada a sua entrada nos casos, e pela maneira, que a Lei determinar. ... XXVII. O Segredo das Cartas é inviolavel. A Administração do Correio fica rigorosamente responsavel por qualquer infracção deste Artigo.

[437] 1891: Art. 72 ... § 18 - É inviolável o sigilo da correspondência. ... § 11 - A casa é o asilo inviolável do indivíduo; ninguém pode aí penetrar de noite, sem consentimento do morador, senão para acudir as vítimas de crimes ou desastres, nem de dia, senão nos casos e pela forma prescritos na lei.

[438] 1934: Art. 113 ... 8) É inviolável o sigilo da correspondência. ... 16) A casa é o asilo inviolável do indivíduo. Nela ninguém poderá penetrar, de noite, sem consentimento do morador, senão para acudir a vítimas de crimes ou desastres, nem de dia, senão nos casos e pela forma prescritos na lei.

[439] 1937: Art. 122 ... 6º) a inviolabilidade do domicílio e de correspondência, salvas as exceções expressas em lei.

[440] 1946: Art. 141 ... § 6º - É inviolável o sigilo da correspondência. ... § 15 - A casa é o asilo inviolável do indivíduo. Ninguém, poderá nela penetrar à noite, sem consentimento do morador, a não ser para acudir a vitimas de crime ou desastre, nem durante o dia, fora dos casos e pela forma que a lei estabelecer.

[441] 1967: Art. 150 ... § 9º - São invioláveis a correspondência e o sigilo das comunicações telegráficas e telefônicas. ... § 10 - A casa é o asilo inviolável do indivíduo. Ninguém pode penetrar nela, à noite, sem consentimento do morador, a não ser em caso de crime ou desastre, nem durante o dia, fora dos casos e na forma que a lei estabelecer.

[442] 1967 após a EC 1/69: Art. 153 ... § 9º É inviolável o sigilo da correspondência e das comunicações telegráficas e telefônicas. § 10. A casa é o asilo inviolável do indivíduo; ninguém pode penetrar nela, à noite, sem consentimento do morador, a não ser em caso de crime ou desastre, nem durante o dia, fora dos casos e na forma que a lei estabelecer.

4.1 Intimidade, vida privada e o sigilo das comunicações na Constituição de 1988

4.1.1 Esclarecimentos terminológicos

Para introduzir a abordagem dos dispositivos constitucionais brasileiros voltados para a proteção da intimidade, a vida privada e do sigilo das comunicações, importa distinguir os conceitos de regras e princípios.

A doutrina demonstra o quão relevante pode ser o acerto no momento de se proceder a tal diferenciação. Para Alexy (2011), mais do que mero conceitualismo teórico, a distinção entre princípios e regras constitui, simplesmente, uma das colunas-mestras do edifício da teoria dos direitos fundamentais, sem a qual não poderia haver nem uma teoria adequada sobre as restrições a direitos fundamentais, nem uma doutrina satisfatória sobre colisões, nem uma teoria suficiente sobre o papel dos direitos fundamentais no sistema jurídico[443].

Sob o chamado critério da generalidade, Alexy diz que princípios ostentam um alto grau de generalidade, enquanto as regras ostentam um baixo grau[444] e menciona diversos outros critérios e teses, adotando o entendimento de que a diferença entre regras e princípios seria qualitativa[445], sendo princípios *mandamentos de otimização*, caracterizados por poderem ser satisfeitos em diferentes graus, e regras normas que só podem ser satisfeitas ou não satisfeitas, fazendo-se valer aquilo que elas determinam, nem mais, nem menos[446].

Segundo Alexy, essa distinção fica mais clara em casos de colisões entre princípios e de conflitos entre regras[447]. O conflito entre regras pode ser resolvido com a introdução de uma cláusula de exceção numa das regras ou, se o método não resolver, com a declaração de invalidade de uma das regras, extirpando-a do ordenamento jurídico[448]. E qual seria, nesse caso, a regra a ser invalidada? Essa questão se solucionaria por meio de regras como *lex*

---

[443] ALEXY, 2011, p. 85. Acrescenta Alexy (p. 87) que não raro são utilizados, em vez de *regra* e *princípio*, *norma* e *princípio* ou *norma* e *máxima*. Lembra que, no precedente *BVerfGE* 51, 324 (350), do Tribunal Constitucional Federal Alemão, usou-se "normas e princípios da Constituição".
[444] Ibid., p. 87.
[445] Dentre os tantos critérios, o autor menciona a determinabilidade dos casos de aplicação, a forma de seu surgimento, o caráter explícito de seu conteúdo axiológico, a referência à ideia de direito ou a uma lei jurídica suprema, a importância para a ordem jurídica. Diferencia princípios e regras, ainda, com base no fato de os primeiros serem razões para os segundos, bem como no fato de os primeiros serem normas de argumentação e os últimos normas de comportamento (ALEXY, 2011, p. 87/89).
[446] ALEXY, 2011, p. 90/91.
[447] Ibid., p. 91.
[448] Ibid., p. 92.

posterior derogat legi priori e *lex specialis derogat legi generali* e também de acordo com a importância das regras em conflito. No caso da colisão entre princípios, verifica-se a precedência nas circunstâncias concretas, a chamada precedência condicionada[449]. O Tribunal Constitucional Federal alemão trata as normas de direitos fundamentais como princípios, conforme se extrai dos sopesamentos de interesses promovidos em diversos casos, nos quais o Tribunal formulou mandamentos de otimização. Exemplos são o caso do Partido Comunista Alemão (*BVerfGE* 5, 85 (204) "o desenvolvimento de sua personalidade na maior medida possível"); o caso das farmácias (*BVerfGE* 7, 377 (403) "a escolha da profissão ... deve ser protegida o máximo possível contra intervenções dos poderes estatais"); e o que regulou os ofícios manuais (*BVerfGE* 13, 97 (195) "a maior liberdade possível na escolha da profissão")[450].

Virgílio Afonso da Silva (2010) aponta como principal traço distintivo ente regras e princípios, segundo a teoria dos princípios, a estrutura dos direitos assegurados pela norma em questão. Nesse sentido, as regras garantiriam direitos (ou imporiam deveres) definitivos, devendo, por isso, ser esses direitos realizados totalmente, desde que – é claro – seja a regra aplicável ao caso concreto. Já os princípios garantiriam direitos (ou imporiam deveres) *prima facie*, devendo esses direitos, portanto, ser realizados apenas parcialmente, devido ao longo caminho existente entre aquilo que é garantido (ou imposto) *prima facie* e aquilo que é garantido (ou imposto) definitivamente[451].

Gilmar Mendes, Inocêncio Coelho e Paulo Gustavo Gonet Branco (2008) observam que se trata de distinção que representa um gerador de importantes efeitos na interpretação e na aplicação das constituições. Se ocorrem os fatos descritos na hipótese de incidência das regras, suas prescrições incidirão necessariamente sobre esses fatos, regulando-os na exata medida do que estatuírem e afastando outras regras concorrentes ou que entrem em conflito com ela[452]. Enquanto as regras dizem como se deve ou não agir em situações específicas, os princípios a esse respeito nada dizem, embora proporcionem critérios para tomar posição em circunstâncias só aparentemente indeterminadas[453]. E os princípios, ao contrário das regras, seriam definidos justamente por não contarem com uma hipótese de incidência e uma consequência jurídica abstratamente determinadas[454].

---

[449] Ibid., p. 93.
[450] Ibid., p. 94.
[451] SILVA, Virgílio Afonso da. **Direitos fundamentais**: conteúdo essencial, restrições e eficácia. 2ª ed. São Paulo: Malheiros, 2010, p. 45.
[452] MENDES; COELHO; BRANCO, 2008, p. 31.
[453] Ibid., p. 38.
[454] Ibid., p. 33.

Para Canotilho (2000), regras são normas que, verificados determinados pressupostos, exigem, proíbem ou permitem algo em termos definitivos, enquanto princípios são normas que exigem a realização de algo da melhor forma possível, de acordo com as possibilidades fáticas e jurídicas[455].

Para o constitucionalista português, a distinção entre regras e princípios faz-se através dos critérios do grau de abstração, do grau de determinabilidade na aplicação do caso concreto, do caráter de fundamentalidade no sistema das fontes de direito, da proximidade da ideia de direito e da natureza normogenética. Pelo primeiro critério, os princípios seriam normas com um grau de abstração maior do que o das regras. Pelo segundo, os princípios, por serem vagos e indeterminados, careceriam de mediações concretizadoras, por parte do legislador e do juiz, enquanto as regras são suscetíveis de aplicação direta. Pelo critério relativo ao caráter da fundamentalidade, os princípios são normas de natureza estruturante ou com um papel fundamental no ordenamento jurídico devido à sua posição hierárquica no sistema das fontes ou à sua importância estruturante dentro do sistema jurídico, a exemplo do princípio do Estado de Direito. Segundo o critério da proximidade da ideia de direito, princípios são *standards* juridicamente vinculantes, radicados na existência de justiça ou de direito, enquanto as regras podem ser normas vinculativas com um conteúdo meramente funcional. Pelo critério da natureza normogenética, os princípios são fundamentos das regras, ou seja, são normas que estão na base ou constituem a *ratio* de regras jurídicas, desempenhando, por isso, uma função normogenética fundamentante[456].

A Constituição brasileira previu, nos incisos X e XII de seu artigo 5º, respectivamente, que "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" e que "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".

É por isso que afirmamos que a norma inscrita no artigo 5º, inciso X, atinente à inviolabilidade da intimidade e da vida privada, é um princípio, e a do inciso XII, atinente à inviolabilidade do sigilo das comunicações, é uma regra.

Afinal, a norma do inciso X é um mandamento de otimização a ser seguido pelo legislador e pelo juiz, mas que também se percebe ter sido seguido pelo próprio constituinte quando redigiu o inciso XII, que contém regra fundamentada na *força normogenética* do

[455] CANOTILHO, 2000, p. 1255.
[456] Ibid., p. 1160/1161.

inciso X. Também o grau de generalidade e de abstração é claramente maior na norma do inciso X do que na do inciso XII. Ademais, se a norma do inciso X fosse uma regra, só poderia ser satisfeita ou insatisfeita de modo total, o que importaria, uma vez assumindo se tratar de norma válida, na impossibilidade absoluta de se admitir qualquer atuação estatal que dependesse do acesso a dados íntimos ou privados do indivíduo, gerando situação que afrontaria até mesmo o senso comum.

O inciso XII contém norma disciplinando como agir em situação específica, ou seja, afirma que o Estado ou quem quer que seja não poderá violar o sigilo de determinadas formas comunicativas, exceto se preenchida a cláusula de exceção inserida na parte final do dispositivo. Já a norma do inciso X se limita a fornecer critério para tomar posição sobre o assunto, sem nada dispor quanto a situações específicas.

A norma do inciso X, ademais, depende de mediações concretizadoras para que possa ser aplicada aos casos concretos, pois não contém, em si mesma, grau suficiente de determinabilidade. Já a do inciso XII traz elementos bastantes para viabilizar seu cumprimento imediato e antes mesmo da edição da lei ordinária por ela prescrita (9.296/96), ao menos no que se refere à obrigação do Estado de se abster de violar o sigilo daquelas modalidades comunicativas.

4.1.2 A regra da inviolabilidade do sigilo das comunicações: restrições[457] e âmbito de proteção

O estudo de direito constitucional mostra que, para se falar em restrições a um direito fundamental, é preciso, antes, se compreender o âmbito de proteção desse direito ou, como prefere Canotilho (2000), o seu âmbito normativo[458], o que também é necessário para se poder avançar num estudo sobre colisões e conflitos entre direitos, pois, muitas vezes, cogita-se

[457] Além de normas de restrição, ou seja, as que limitam ou restringem posições que, *prima facie*, se incluem no domínio de proteção dos direitos fundamentais, a doutrina constitucional fala em normas de conformação de um direito fundamental, como aquelas que completam, precisam, concretizam ou definem o conteúdo de proteção de um direito fundamental (CANOTILHO, 2000, p. 1263). Não se tratará aqui destas últimas, pois a regra do artigo 5º, inciso XII da CF, prescreveu ao legislador a edição de norma infraconstitucional restritiva, o que foi feito através da Lei 9.296/96.

[458] CANOTILHO, 2000, p. 1262.

suposta colisão entre direitos, mas a conduta está, na realidade, fora do âmbito de proteção do direito[459].

Como nem sempre é simples a verificação se determinado direito fundamental contempla determinados comportamentos e realidades da vida (exemplos: se curandeirismo se ampara na liberdade de culto; se o discurso de ódio racial é tutelado pela liberdade de expressão), os critérios para resolver essas indeterminações e aferir a limitação intrínseca da norma de direito fundamental são vários e podem ser combinados: teoria liberal dos direitos fundamentais (assinala nesses direitos a feição essencialmente de defesa do indivíduo contra os poderes públicos); teoria dos valores (postula que os direitos fundamentais possuem caráter objetivo, orientando-se para a realização dos valores protegidos pela norma constitucional); consideração da função social que o direito proclamado exerce (em especial tendo em vista seu significado para o regime político). Outro critério é verificar se a conduta está definida como crime, o que, apesar do perigo de se definir o direito fundamental a partir do legislador ordinário, tem sido aceito pela doutrina e jurisprudência, desde que com a adoção de cuidados no exame da razoabilidade da apreciação do legislador[460].

Este último critério, por exemplo, levaria à interpretação de que a liberdade de profissão (art. 5º, XIII, CF) não se estende a atividades tipificadas como crime, como contrabando ou tráfico de entorpecentes, pois, se determinada conduta atinge intoleravelmente valores sociais básicos ou princípios fundamentais da ordem constitucional, a ponto de ter sido classificada como ilícito penal, deverá resultar para o intérprete a convicção de que a proteção constitucional de determinado direito não quis ir tão longe[461].

Segundo o critério de Friedrich Müller (1990), a delimitação do conteúdo de um direito fundamental e de seus limites se faz pelo critério da especificidade, pelo qual será específico todo ato que faça parte do âmbito da norma de determinado direito fundamental[462], sendo não específico ou não típico todo ato que pode ser, sem perdas para o exercício típico de um direito fundamental, substituído por outro[463].

---

[459] MENDES; COELHO; BRANCO, 2008, p. 341.
[460] CANOTILHO, 2000, p. 1275/1276; MENDES; COELHO; BRANCO, 2008, p. 289; ANDRADE, José Carlos Vieira de, **Os direitos fundamentais na Constituição portuguesa de 1976**. 5ª ed. Coimbra: Almedina, 2012, p. 276; e, no que se refere à jurisprudência, "*Habeas corpus*. Curandeirismo. Condenação criminal fundada em fatos inconfundíveis com o mero exercício da liberdade religiosa. Processo penal que não se pode invalidar em *habeas corpus*. Recurso desprovido" (BRASIL. Supremo Tribunal Federal. HC 62.240/SP, rel. min. Francisco Rezek, 2ª T., j. 13.12.1984, DJ 02.08.1985).
[461] VIEIRA DE ANDRADE, 2012, p. 276.
[462] MÜLLER, Friedrich, **Die Positivität der Grundrechte**: Fragen einer praktischen Grundrechtsdogmatik. 2ª ed., Berlin: Duncker & Humblot, 1990, p. 64, 73, 74, 88, 93 e 98 apud SILVA, V. A. da, 2010, p. 88.
[463] MÜLLER, 1990, p. 101 apud SILVA, V. A. da, 2010, p. 88.

Virgílio Afonso da Silva (2010), lidando com o que chamou de "circularidade d[esta] definição", dela extrai que toda e qualquer ação que não seja estruturalmente necessária ao exercício do direito fundamental e que, nesse sentido, possa ser substituída por outra é uma ação não específica e, portanto, não protegida pelo direito fundamental[464].

Sobre a tarefa de definir o que é específico de um direito, Gilmar Mendes, Inocêncio Coelho e Paulo Gonet Branco (2008) falam na distinção entre o que é exercício de um direito fundamental e o que seria uma circunstância meramente acidental de seu exercício[465].

Num primeiro exemplo célebre, Müller (1990) afirma que a proibição a que um cientista divulgue suas teses através de cartazes em prédios públicos ou autofalantes não seria uma restrição ao direito fundamental à liberdade científica, já que tais formas de divulgação não são típicas ou específicas. Afinal, poderão ser substituídas pela publicação das mesmas teses numa revista científica, nos moldes tradicionais[466]. Num segundo exemplo, também clássico, Müller (1969) afirma que o mesmo se poderia dizer do artista que pretendesse pintar um quadro no meio de um cruzamento movimentado, pois, embora a ação de pintar quadros seja protegida pela liberdade artística, sua forma de exercício, em um cruzamento viário, não é específica ou típica dessa liberdade, podendo ser substituída por outra[467].

Afinal, proibir um pintor de se instalar num cruzamento esvaziaria a garantia da liberdade artística? Esta permissão é condição *sine qua non* para seu exercício? A resposta é evidentemente negativa, o que leva à conclusão de que tal conduta não está alcançada pelo âmbito de proteção do direito de liberdade artística.

A crítica a esse critério é a de que poderia acontecer que nada, nenhuma ação sobrasse de específica em relação a um direito fundamental[468].

Mendes, Coelho e Branco (2008) observam, também, que o âmbito de proteção não pode ser fixado em regras gerais, sendo necessário para cada direito um procedimento, o que, muitas vezes, exigirá uma interpretação sistemática, considerando outros direitos e disposições constitucionais, somente sendo possível determinar o âmbito de proteção em confronto com eventual restrição a esse direito[469].

Segundo Canotilho (2000), para identificar o âmbito, primeiramente analisa-se a estrutura da norma constitucional garantidora de direitos, buscando-se determinar quais os

---

[464] SILVA, V. A., 2010, p. 88.
[465] MENDES; COELHO; BRANCO, 2008, p. 290.
[466] MÜLLER, 1990, p. 101 apud SILVA, V. A. da, p. 88.
[467] MÜLLER, **Freiheit der Kunst als Problem der Grundrechtsdogmatik**, Berlin: Duncker & Humblot, 1969, p. 59 apud SILVA, V. A., 2010, p. 88/89.
[468] MENDES; COELHO; BRANCO, 2008, p. 290.
[469] Ibid, p. 296.

bens jurídicos protegidos e qual a extensão dessa proteção; e verifica-se, em seguida, se há alguma restrição imediatamente estabelecida pela própria constituição (restrição constitucional expressa) ou se a constituição autoriza a lei a restringir esse âmbito de proteção (reserva de lei restritiva)[470].

Dito isto, tem-se que do direito à privacidade e à intimidade previstos na Constituição (art. 5º, X) já emanaria um direito à inviolabilidade do sigilo das comunicações, ainda que este não contasse com previsão autônoma, como conta (art. 5º, XII).

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 caso do direito à inviolabilidade do sigilo das comunicações no Brasil, há reserva de lei restritiva por imposição da própria Constituição (art. 5º, XII da CF), ocorrendo a chamada técnica de restrição legal mediata, pela qual o texto constitucional transfere ao legislador infraconstitucional o dever de estabelecer as restrições ao direito. É o que ocorre também com o livre exercício profissional (inciso XIII), com a liberdade de locomoção (inciso XV) e com a liberdade de associação (inciso XVII)[471]. Classificação semelhante é a adotada por Alexy (2011), para quem há as restrições diretamente constitucionais e as indiretamente constitucionais, sendo as primeiras aquelas estabelecidas no próprio texto constitucional e as últimas aquelas feitas por obra do legislador infraconstitucional[472].

Essa incumbência transferida pelo constituinte ao legislador pode se dar de duas formas, dando causa à existência de outra classificação. Haverá *restrição legal simples* ou *reserva legal simples* quando o constituinte se limitar a autorizar a intervenção do legislador, sem fazer qualquer exigência quanto ao conteúdo ou finalidade da lei (usam-se, por exemplo, expressões como "na forma da lei", "nos termos da lei", "salvo nas hipóteses previstas em lei" ou "no prazo da lei"). Por outro lado, se estará diante de caso de *restrição legal qualificada* ou *reserva legal qualificada* quando o constituinte balizar a intervenção da lei ordinária, fixando-lhe determinado objetivo ou requisito constitucional expresso[473].

---

[470] CANOTILHO, 2000, p. 1275.

[471] Já na chamada técnica de estabelecimento direta, a própria Constituição estabelece restrições a direitos fundamentais, tal qual ocorre com o inciso XI do artigo 5º, que afasta diretamente a inviolabilidade do domicílio em caso de flagrante, desastre e ordem judicial, durante o dia, e com o inciso XVI, que condiciona o direito de reunião em locais públicos à ausência de armas (MENDES; COELHO; BRANCO, 2008, p. 299/300 e 302).

[472] ALEXY, 2011, p. 285/286. Ressalva-se, contudo, o entendimento da chamada teoria externa (*Aussentheorie*), segundo a qual, não há restrições estabelecidas pela própria Constituição, mas apenas limitações, que são a própria definição do direito, ao passo que, para a teoria interna (*Innentheorie*), pode haver, sim, na Constituição, o direito assegurado e, no mesmo ou noutro dispositivo, sua eventual restrição (ALEXY, 2011, p. 276/277).

[473] MENDES; COELHO; BRANCO, 2008, p. 306.

Esta última modalidade, da reserva legal qualificada, é a que ocorre com a inviolabilidade do sigilo das comunicações estabelecida no inciso XII do artigo 5º, pois a expressão "*nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal*" nada mais é do que uma prescrição do constituinte ao legislador ordinário, balizada por critérios específicos[474]. No caso, a imposição constitucional é a de que as situações em que será possível afastar o sigilo das comunicações precisarão ter sua forma e hipóteses previstas em lei e tal afastamento precisará se destinar a investigação criminal ou instrução processual penal.

Por isso, aliás, o STF julgou não recepcionado o artigo 57, II da Lei 4.117/62 (Código Brasileiro de Telecomunicações)[475], que admitia a violação de telecomunicação mesmo na ausência de lei estabelecendo as hipóteses de cabimento da medida.

Observa-se uma divergência doutrinária apresentada por Alexy (2011) quanto a duas concepções existentes sobre as restrições ou limites a direitos fundamentais. Pela chamada teoria externa, existiria o direito em si, concebido sem restrição, e, em segundo lugar, existiria a restrição. Já pela teoria interna, não haveria duas coisas (o direito ilimitado e a restrição que sobre ele incide), mas apenas uma, qual seja, o direito com um determinado conteúdo, substituindo-se o conceito de restrição pelo de limite ou de *restrição imanente*[476].

Virgílio Afonso da Silva (2010) explica a teoria interna como o enfoque a partir do qual o processo de definição dos limites de cada direito é algo interno a ele, donde se concebe a figura dos *limites imanentes*, ou seja, pela teoria interna, existe apenas um objeto: o direito com seus limites imanentes, não sendo esses limites definidos ou influenciados por qualquer aspecto externo, sobretudo não por colisões com outros direitos[477]. Já na teoria externa haveria dois objetos: o direito em si e, destacadas dele, as suas restrições[478].

Diz Alexy (2011) que, longe de se tratar de mera diferença teórica, a opção pela teoria externa revelará, por parte do intérprete, a adoção de uma concepção individualista do Estado e da sociedade, enquanto que a opção pela teoria interna revelará que o mais importante no indivíduo é seu papel de membro ou participante de uma comunidade[479].

---

[474] A Constituição, no entanto, trouxe algumas restrições imediatas a essa inviolabilidade, a saber, no regime excepcional do estado de necessidade (defesa e sítio), em que podem ser estabelecidas restrições especiais ao direito de reunião, ao sigilo de correspondência e comunicação telegráfica e telefônica (art. 136, §1º, I, a-c, CF) e comunicação em geral (art. 139) (MENDES; COELHO; BRANCO, 2008, p. 303).
[475] BRASIL. Supremo Tribunal Federal. HC 69912/RS, rel. min. Sepúlveda Pertence, Pleno, j. 16.12.1993, DJ 25.03.1994.
[476] ALEXY, 2011, p. 277/278.
[477] SILVA, V. A., 2010, p. 128.
[478] Ibid., p. 138.
[479] ALEXY, 2011, p. 278.

Concordamos com a constatação de Virgílio Afonso da Silva (2010), no sentido de que, em face da impossibilidade da existência de direitos absolutos – e o próprio conceito de mandamento de otimização já prevê que a realização de um princípio pode ser restringida por princípios colidentes –, a definição do conteúdo definitivo de um direito é estabelecida a partir de fora, a partir de condições fáticas e jurídicas existentes[480].

Assume-se no presente trabalho, portanto, a teoria externa, que, ademais, se mostra a mais coerente com os objetivos primordiais dos direitos fundamentais, no sentido de que, para usar como exemplos os direitos ora sob análise, a inviolabilidade da intimidade e da vida privada (art. 5º, X da CF) são direitos concebidos sem qualquer restrição, voltados para proteger o indivíduo na maior extensão possível e, se o indivíduo não invadisse a esfera de proteção de outro indivíduo ou outros interesses sociais, sua proteção deveria ser, hipoteticamente, assegurada de modo absoluto. O mesmo deverá ocorrer com o direito à inviolabilidade do sigilo das comunicações (art. 5º, XII da CF) que, salvo se houver preenchimento da cláusula de exceção inserida na parte final do dispositivo, deve ser concebido como um direito sem restrições. Portanto, adota-se a teoria externa, assumindo-se que existem, de um lado, os direitos fundamentais e, de outro, as restrições, que decorrem dos demais direitos fundamentais e das normas protetivas de interesses da comunidade.

Mas, segundo bem colocado por Alexy (2011), o conceito de restrição a um direito parece familiar e não problemático, sendo esta uma ideia até natural e trivial, residindo o problema, na verdade, em definir o conteúdo e a extensão dessas restrições[481], o que, noutras palavras, definirá o âmbito de proteção do direito fundamental sob estudo.

No caso da inviolabilidade do sigilo das comunicações (art. 5º, XII da CF), a restrição legal qualificada se deu através da Lei 9.296 de 1996, sendo certo que ela, como qualquer outro diploma infraconstitucional que se pretenda restritivo de um direito fundamental, precisa ser uma norma compatível com a Constituição[482], sob pena de a pretendida restrição se transfigurar em violação.

Dito de outro modo, o legislador, ainda que incumbido pela Constituição de fixar restrições a direitos fundamentais, não poderá, por óbvio, ultrapassar uma certa margem de segurança, já que há, naturalmente, um limite de atuação do legislador infraconstitucional, de modo a que este não possa, com restrições arbitrárias ou aleatórias, esvaziar um direito individual estabelecido pela Constituição. E o instrumento a se recorrer para avaliar a

[480] SILVA, V. A., 2010, p. 140.
[481] ALEXY, 2011, p. 276.
[482] Ibid., p. 281.

aceitabilidade dos níveis de restrição que uma norma gera a um direito fundamental é o princípio da proporcionalidade, introduzido no item 1.4, *supra*, e que servirá de base às conclusões que buscaremos no presente capítulo.

Rememorando-se os conceitos espanhóis de comunicação em *canal abierto* e comunicação em *canal cerrado*[483], envolvendo meios de comunicação, respectivamente, sem e com restrição a um grupo específico de destinatários escolhidos, resta evidente que as comunicações travadas em *canal abierto* estão fora do âmbito de proteção do direito à inviolabilidade do sigilo das comunicações.

Nesse sentido, Juan López (2012) observa que "*desde el punto de vista subjetivo, no es intervención de las comunicaciones la obtención de información por uno de lós interlocutores, a menos que se emplee a éste instrumentalmente. Es el caso de los datos obtenidos por los agentes de policía en comunicaciones en canal abierto (chats, redes peer to peer, etc.), pero también en comunicaciones en canal cerrado cuando son interlocutores*"[484].

No entanto, há, neste ponto, questão mais tormentosa e de conclusões não tão óbvias, qual seja, a da inserção ou não, neste âmbito de proteção, da comunicação travada com um grupo de destinatários grande, porém não indefinido a ponto de ser classificado como de *canal abierto*. Classificaremos como comunicação em *canal semiaberto* aquela dirigida a um grupo numeroso, mas não indeterminado, de pessoas conscientemente escolhidas pelo remetente.

A comunicação em canal semiaberto não deixa de ser uma comunicação fechada, porém a inclusão de um grande número de destinatários, que quantificamos em vinte, seja num e-mail, seja num *site* de relacionamento, seja num *chat*, importa, a nosso ver, em declínio tácito do direito ao sigilo, não importando eventual acesso do Estado àquele conteúdo em violação do sigilo de comunicações. A tal conclusão se chega em razão de o remetente, ao incluir tantos destinatários numa comunicação, estar agindo sem expectativa de privacidade[485] ou com expectativa de privacidade tão reduzida, a ponto de igualá-la àquela incidente sobre as comunicações em *canal abierto*, excluindo-se a conversa do âmbito de proteção do direito ao sigilo das comunicações. Dito de outro modo, seria como situar aquela comunicação fora do círculo concêntrico da intimidade e, mais do que isso, fora também do próprio círculo, mais amplo, da privacidade[486].

---

[483] Ver item 3.3.1.
[484] LÓPEZ, 2012, p. 118/119.
[485] O conceito de expectativa de privacidade (*expectation of privacy*) emana da jurisprudência norte-americana, conforme retratado no item 3.1.1.
[486] Abordamos a teoria dos círculos concêntricos no item 1.1.

4.1.3 A inviolabilidade do sigilo das comunicações e as exceções constitucionais

Não é tarefa fácil definir quais são as formas de comunicação cuja inviolabilidade foi excepcionada pelo constituinte.

Observa-se, no entanto, uma prevalência do entendimento doutrinário de que a exceção constitucional à regra da inviolabilidade absoluta das comunicações só se aplicaria à quarta modalidade, "comunicações telefônicas".

Neste sentido, veja-se que, para Ada Pellegrini Grinover, Antonio Magalhães Gomes Filho e Antonio Scarance Fernandes (2009), no que se refere à interceptação de correspondência, comunicação de dados e telegráfica, a Constituição estabeleceu a inviolabilidade absoluta do sigilo[487].

Luiz Francisco Torquato Avolio (2010) defende que, da redação empregada pelo legislador constituinte no que se refere às interceptações não telefônicas, deflui "uma colocação em termos absolutos", já que "a própria Constituição já estabelece expressamente a exceção, e – por força de estrita interpretação gramatical e lógica – a única exceção que pretendia impor à regra do sigilo da correspondência e das comunicações"[488].

Lenio Streck (2001) afirma não ter dúvida de que a exceção constitucional contempla apenas a interceptação telefônica, mas entende que é possível a interceptação do tráfego de toda e qualquer informação que se utilize da modalidade "comunicações telefônicas", aí incluída aquela realizada através de sistemas de informática, existentes ou que venham a ser criados[489]. O autor, no entanto, parte da premissa de que toda espécie de comunicação de dados se serve de linhas telefônicas, o que não corresponde à realidade, já que existem hoje inúmeras outras modalidades de conexão não baseadas em telefonia, a exemplo de cabos de sinal de televisão, frequência de rádio e cabos dedicados de internet.

Semelhantemente, para Luiz Flavio Gomes e Raul Cervini (1997), a interceptação telemática, que definiram como o uso combinado de telefone e informática, seria possível porque a comunicação "*modem by modem*" ou via internet, no fundo, não passaria de uma

---

[487] GRINOVER; GOMES FILHO; FERNANDES, 2009, p. 167/168.
[488] AVOLIO, Luiz Francisco Torquato. **Provas ilícitas**: interceptações telefônicas, ambientais e gravações ambientais. 4ª ed. São Paulo: Revista dos Tribunais, 2010, p. 170.
[489] STRECK, Lenio Luiz. **As interceptações telefônicas e os direitos fundamentais**. 2ª. ed. Porto Alegre: Livraria do Advogado, 2001, p. 46/47.

comunicação telefônica. Entender o contrário, segundo sustentam, constituiria num "enorme atraso tecnológico-cultural", que acabaria por inviabilizar a investigação do criminoso da era digital e do crime organizado, que já não funciona sem o uso da informática[490].

Já Greco Filho (2005), invocando o sigilo como regra e a interceptação como exceção, sustenta que a expressão "no último caso", dentro das possíveis interpretações gramaticais, só se refere à interceptação telefônica, cujo significado o autor não admite confundir-se com comunicação por meio de linha telefônica, pois, se a Constituição quisesse tal extensão, teria usado a expressão "comunicação por rede telefônica" ou "por linha telefônica", o que não fez[491].

A esse respeito, Gustavo Badaró (2010) observa que o tratamento da comunicação telemática como, tão simplesmente, uma modalidade da comunicação telefônica seria equivocado, vez que a própria Lei Geral das Comunicações, a Lei 9472/97, distinguiu as formas de telecomunicações em "a telefonia, a telegrafia, a comunicação de dados e a transmissão de imagens" (art. 69, § único)[492].

Gilmar Mendes, Inocêncio Coelho e Paulo Gustavo Gonet Branco (2008) reconhecem que a leitura do preceito constitucional do artigo 5º, inciso XII pode levar à conclusão de que apenas nos casos de comunicações telefônicas seria possível a quebra do sigilo, restando este absoluto em relação aos dados constantes de correspondência postal, telegráfica ou de comunicações telemáticas. Apesar disso, os três autores sustentam que a restrição de direitos fundamentais poderia ocorrer mesmo sem autorização expressa do constituinte, sempre que se fizesse necessária a concretização do princípio da concordância prática entre ditames constitucionais[493], já que, diante de não serem absolutos, o direito à inviolabilidade do sigilo das correspondências e das comunicações telegráficas poderia ser restringido em casos recomendados pelo princípio da proporcionalidade[494].

Há outra forma de interpretação que lê o dispositivo constitucional do inciso XII do artigo 5º como contendo duas partes. A primeira afirmaria a inviolabilidade do sigilo "da correspondência e das comunicações telegráficas" e a segunda afirmaria a "de dados e das

---

[490] GOMES; CERVINI. 1997, p. 167 e 169.

[491] GRECO FILHO, Vicente. **Interceptação telefônica**: considerações sobre a Lei n. 9.296, de 24 de julho de 1996. 2ª ed. rev., atual. e ampl. (com a colaboração de João Daniel Rassi). São Paulo: Saraiva, 2005, p. 15/17.

[492] BADARÓ, 2010, p. 488.

[493] Trata-se de princípio, também chamado de princípio da harmonização, pelo qual se recomenda ao intérprete, quando se deparar com situações de concorrência entre bens constitucionalmente protegidos, adote a solução que otimize a realização de todos eles, mas ao mesmo tempo não acarrete a negação de nenhum (MENDES; COELHO; BRANCO, 2008, p. 114). Reconhecem os autores, no entanto, que se trata de uma conciliação puramente formal ou principiológica, pois nas demandas reais só um dos contendores terá acolhida, por inteiro ou em grande parte, a sua pretensão (p. 114/115).

[494] MENDES; COELHO; BRANCO, 2008, p. 392.

comunicações telefônicas", de modo a que a ressalva "no último caso" se referiria às comunicações de dados e telefônicas, estando, portanto, ambas sujeitas a afastamento "por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal".

Trata-se da corrente *intermediária*, havendo, também, a *restritiva*, que só admite as interceptações telefônicas, e *ampliativa*, que admite a interceptação das correspondências e das comunicações telegráficas, telefônicas e de dados[495-496].

Também para Tércio Sampaio Ferraz (1993), a Constituição assegura o sigilo de dados relativamente à comunicação, no interesse da defesa da privacidade[497], o que se faria em dois blocos: o do sigilo da correspondência e comunicações telegráficas e o do sigilo de dados e das comunicações telefônicas[498]. O autor observa que, dos quatro meios de comunicação ali mencionados, ou seja, correspondência, telegrafia, dados e telefonia, só o último se caracteriza por sua instantaneidade, ou seja, é a única que não deixa vestígios, sendo a interceptação sub-reptícia a única forma de se preservar o conteúdo da comunicação[499].

No que se refere, por exemplo, à movimentação bancária de um indivíduo, Tércio Ferraz, seguindo sua linha de raciocínio, sustenta que a movimentação pode ser acessada pelas autoridades, em nome do interesse público, mas não poderá sê-lo a própria ação comunicativa[500].

Gustavo Badaró (2010), no entanto, percebe que uma das premissas que lastrearam o raciocínio de Tércio Ferraz e do constituinte de 1988 foi a de que a comunicação de dados necessariamente deixava vestígios, o que, hoje, após mais de duas décadas de evolução tecnológica, já não é uma realidade[501], pois diversas são as formas de comunicação de dados que não geram o armazenamento do teor do diálogo[502].

De fato, como observa o autor português Benjamim Silva Rodrigues (2009), nesta era dos fluxos informacionais e comunicacionais digitais, a prova física dá lugar à prova digital, fazendo com que o que realmente importe sejam os *bits* e os *bits-acerca-dos-bits*, provocando

---

[495] MACHADO, André Augusto Mendes; KEHDI, Andre Pires de Andrade. Sigilo das comunicações de dados. In: FERNANDES, Antonio Scarance; ALMEIDA, José Raul Gavião de; MORAES, Maurício Zanoide de (Coord.). **Sigilo no processo penal**: eficiência e garantismo. São Paulo: Revista dos Tribunais, 2008, p. 243/245.
[496] Da mesma forma se pronunciou o STF (BRASIL. Supremo Tribunal Federal. Pet-QO 577/DF, rel. min. Carlos Velloso, Pleno, j. 25.03.1992, DJ 23.04.1993, voto do ministro Marco Aurélio, em folhas 19 a 22).
[497] Segundo o autor, como vimos, intimidade se liga a aspectos não compartilhados com absolutamente ninguém.
[498] FERRAZ JR., 1993, p. 446.
[499] Ibid., p. 447/448.
[500] Ibid., p. 452.
[501] BADARÓ, 2010, p. 490.
[502] Pode-se citar o Skype e o MSN quando utilizados na modalidade de voz (não escrita) e o VoIP.

verdadeira erosão na eficácia dos meios clássicos de obtenção da prova[503] talhados para o mundo físico[504].

Geraldo Prado (2006) se posiciona no mesmo sentido de Tércio Ferraz, entendendo que a interpretação sistemática e teleológica da Constituição levaria à admissibilidade da interceptação de dados para fins de investigação penal e instrução processual penal, quando não se estiver diante de dados que virão a repousar em bancos de dados, de modo a se tornarem passíveis de apreensão posterior[505].

Para Gustavo Badaró (2010), tal raciocínio é correto, porém com premissas mutáveis conforme evolui a tecnologia das comunicações, razão pela qual o objeto de análise não deve ser o meio de comunicação utilizado, mas sim o processo comunicante[506], a partir do qual se pode constatar se o teor das comunicações se pereniza de alguma forma e se, desta forma, é passível de apreensão. É diante disso que Badaró afirmou que e-mail (que se pereniza) se sujeita à inviolabilidade absoluta[507], tendo observado que a restrição de um direito fundamental não deve ser balizada por comodismo ou mesmo por uma busca de máxima eficiência da persecução penal[508].

Essa interpretação aparenta se mostrar consentânea com o princípio da *ultima ratio*, na medida em que só se poderá violar o sigilo de comunicações quando não houver meio menos gravoso de se obter a prova, como, por exemplo, através da apreensão dos registros perenizados das conversações. Esta, aliás, como visto acima, é uma das exigências do princípio da proporcionalidade em seu subprincípio necessidade, que impõe ao Estado a adoção da medida menos onerosa possível para os direitos fundamentais do indivíduo[509].

Entendemos, no entanto, de forma diversa, para o que invocamos dois raciocínios judiciais adotados para aspectos que tangenciam este ponto do tema. Vislumbramos, aqui, ademais, um atendimento, de fato, à exigência de se adotar a medida menos gravosa e onerosa para o indivíduo, porém tal medida, a nosso ver, de tornar a comunicação via e-mail arrecadável exclusivamente por meio de apreensão física, não se mostra apta a obter o fim pretendido para realizar o interesse público, pelo que restaria desatendido o subprincípio da adequação.

---

[503] Tratar-se-á dos meios de prova, meios de obtenção de prova e meios de investigação no item 6.2, *infra*.
[504] RODRIGUES, 2009, p. 23.
[505] PRADO, Geraldo. **Limite às interceptações telefônicas e a jurisprudência do Superior Tribunal de Justiça**. 2ª ed. Rio de Janeiro: Lumen Juris, 2006, p. 73.
[506] BADARÓ, 2010, p. 491 (nota de rodapé 26).
[507] Ibid., p. 492.
[508] BADARÓ, 2010, p. 493.
[509] Tratamos do princípio da proporcionalidade no item 1.4.

Pelo primeiro raciocínio, do Tribunal Supremo da Espanha – e aqui já antecipando as conclusões a que chegaremos no item 4.11, quanto aos dados de tráfego de comunicações que se inserem no âmbito de proteção do direito ao sigilo das comunicações –, os dados externos ao processo comunicativo[510] que se inserem no âmbito de proteção de tal direito são aqueles vinculados a comunicações concretamente realizadas, como, por exemplo, os registros de data e horário *de e-mails transmitidos*, os dados de um interlocutor *que se comunicou com o alvo*, a duração *de comunicação que efetivamente aconteceu*[511]. Entendemos que afastar o sigilo sobre tais dados comunicativos do âmbito normativo no inciso XII do artigo 5º iria na contramão do sentido do texto constitucional, na medida em que a crença legítima do indivíduo em que tais dados estarão inacessíveis aos terceiros que ele não tenha escolhido como interlocutores se mostra, pelo princípio da especificidade, evidentemente específica do exercício do direito em questão.

Se aqueles dados externos estão inseridos no âmbito de proteção do direito ao sigilo das comunicações, entendemos que devem se sujeitar ao acesso dos órgãos de investigação segundo o mesmo regime normativo que rege as interceptações. Por outro lado, entendemos que, uma vez apreendidos fisicamente numa busca e apreensão, o acesso a eles dependerá de autorização judicial que deverá atender às mesmas exigências que cercariam uma interceptação.

O mesmo entendemos em relação a "processos comunicantes" (expressão que Gustavo Badaró utilizou, acima) cujos dados de conteúdo humano das comunicações realizadas se perenizem, ou seja, entendemos que, uma vez que eles se inserem no âmbito de proteção do direito ao sigilo das comunicações, poderão ser alvo de interceptação.

Ademais, estágios de perenização das mensagens trocadas por meio de comunicação telemática são uma constante em muitas formas comunicativas modernas, e não só no e-mail. Como abordado no item 3.1.3, o Professor Orin Kerr (2003), da *George Washington University Law School*, observou que a estrutura de funcionamento da internet parece ter sido desenvolvida para excluí-la da esfera de proteção da Quarta Emenda da Constituição norte-americana, que não protege informações que tenham sido divulgadas a terceiros. Isto porque, na internet, ao pressionar a tecla "enviar", a mensagem passa por diversos servidores,

[510] Ver definição de dados externos no item 3.1.4.

[511] Exemplos de dados de tráfego excluídos do âmbito de proteção do direito ao sigilo das comunicações, como concluiremos no item 4.11, são os dados cadastrais de assinantes, tais como seu endereço e telefone, os dados identificadores de aparelhos (a exemplo do código IMEI) e do usuário (a exemplo do IMSI) e o IP do assinante (quando se tratar de IP fixo, porquanto o dinâmico estará sempre vinculado a uma comunicação concretamente realizada, nem que seja apenas uma troca de protocolos de sistema, entre o alvo e seu próprio servidor). Os demais dados externos estarão submetidos ao direito geral à intimidade (art. 5º, X, CF).

provedores e outros computadores, divulgando-a para cada um deles com instruções para encaminhá-la ao seguinte, até a chegada ao destinatário final, de forma a ter seu conteúdo visto por muitos *intermediários* no meio do caminho.

Essa perenização obrigatória, que se dá no meio do caminho de muitas formas de comunicação telemática, é, portanto, inerente à modernização do processo comunicativo – e aqui passamos ao segundo precedente jurisprudencial a subsidiar nosso entendimento.

No caso *United States v. Knotts*, a Suprema Corte dos Estados Unidos afastou a legítima *expectation of privacy* sobre o registro dos números discados por um investigado, na medida em que, com o uso do telefone, ele teria assumido o risco de que a companhia telefônica registrasse os números que discou e os revelasse à polícia, afastando-se, assim, a proteção da Quarta Emenda. Afinal, observou a Suprema Corte, o equipamento que registra os números discados seria tão simplesmente *a versão moderna do operador de telefonia* que, antigamente, colhia os números desejados e completava as ligações para os usuários. Diante do argumento do investigado de que somente se, de fato, se tratasse ainda de um operador humano de antigamente seria razoável se afastar a *expectation of privacy*, a Corte replicou que não seria de se admitir um resultado constitucional distinto só porque a companhia telefônica resolveu se automatizar[512].

De forma análoga, entendemos que não se deve destinar às formas comunicativas que dependem de estágios de perenização para sua completude tratamento constitucional diverso, pelo que concluímos que o e-mail é passível de interceptação e, caso venha a ser arrecadado através de eventual busca e apreensão de um disco rígido, o acesso pelo órgão de investigação aos dados nele preservados dependerá de autorização judicial específica que deverá atender às mesmas exigências de uma interceptação.

Quanto à análise da cláusula de exceção do inciso XII, definir se ela, ao dizer "salvo, no último caso", se refere somente às comunicações telefônicas ou também às de dados ou às duas anteriores e também à telegráfica dependerá da leitura dos métodos hermenêuticos doutrinariamente consagrados[513]. A análise dos elementos filológicos ou gramaticais, que

[512] "We are not inclined to hold that a different constitutional result is required because the telephone company has decided to automate" (United States v. Knotts). Precedente analisado no item 3.1.1.

[513] CANOTILHO, 2000, p. 1210/1214: (1) Pelo método de interpretação jurídica ou método jurídico, no qual se consideram os elementos filológico (literal; gramatical; textual), lógico (sistemático), histórico, teleológico (racional) e genético, dá-se dupla relevância ao texto, que se presta a ser, ao mesmo tempo, ponto de partida para a tarefa de compreender o texto e limite desta tarefa, não podendo o intérprete ir além ou, muito menos, ir contra o teor literal do preceito; (2) Pelo método tópico-problemático, adota-se o caráter prático da interpretação, no sentido de resolver os problemas concretos, partindo da premissa de que a lei constitucional é aberta, fragmentária ou indeterminada. Critica-se este método por poder ocasionar um casuísmo sem limites; (3) Pelo método hermenêutico-concretizador, o intérprete parte de uma situação histórica concreta, concretizando a norma numa atividade prático-normativa de compreender o sentido da norma com preenchimento de sentido

integram o chamado método jurídico de interpretação, não parece em condições de levar o intérprete a nenhum lugar, pois a redação do inciso XII é um exemplo autêntico de ambiguidade linguística, com diversas possibilidades de leitura.

A única certeza que se pode extrair dos aspectos textuais desse dispositivo é que a correspondência epistolar é indubitavelmente inviolável, pois não há a mínima possibilidade de que, com aquela redação, esteja abrangida por uma cláusula de exceção[514].

Já com a leitura dos elementos históricos, racionais, sistemáticos e genéticos da norma, também integrantes do método jurídico, seria possível se progredir na missão, pois é possível se verificar que a realidade histórica das tecnologias comunicativas que inspiraram o constituinte de 1988 não permitia a compreensão visionária do que se tornou o mundo de hoje quanto à multiplicidade e à extrema velocidade dos meios de comunicação e da evolução destes.

Hoje, com um aumento exponencial da utilização dos meios digitais de comunicação, a vida do indivíduo é facilitada, acelerada e beneficiada sob inúmeros aspectos. Mais do que isso, há hoje uma espécie de presunção generalizada de que cem por cento da população mundial (ao menos nos centros urbanos) está on-line, acessível em tempo real através de alguma forma comunicativa, aí incluídos o telefone celular, o *Facebook*, a telefonia fixa, o Skype, o MSN, o e-mail e outras que existem e que virão a existir.

Em contrapartida a essa verdadeira mudança de paradigma nas relações pessoais e profissionais, surge, do lado dos interesses da comunidade, uma necessidade de que os mecanismos existentes para satisfazer o princípio da segurança (art. 5º, *caput* da CF) e os mandamentos de criminalização (art. 5º, XLI, XLII, XLIII e XLIV, art. 7º, X e art. 227, §4º e

---

juridicamente criador. Difere do método tópico-problemático porque enquanto aquele pressupõe ou admite o primado do problema perante a norma, o hermenêutico-concretizador se assenta no pressuposto do primado do texto constitucional em face do problema; (4) O método científico-espiritual, também chamado de valorativo e sociológico se baseia na necessidade de interpretação da Constituição tendo em conta as bases de valoração (a ordem de valores ou sistema de valores) subjacentes ao texto constitucional e o sentido e a realidade da Constituição como elemento do processo de integração; (5) Pela metódica jurídica normativo-estruturante, investigam-se as várias funções de realização do direito constitucional (legislação, administração, jurisdição) para captar a transformação das normas numa decisão prática, pois este método se pretende ligado à resolução de problemas práticos. Essa metódica se preocupa com a estrutura da norma e do texto normativo, com o sentido da normatividade e de processo de concretização, com a conexão de concretização normativa e com as funções jurídico-práticas; (6) Pelo método da interpretação comparativa, capta-se, de forma jurídico-comparatística, a evolução da conformação, diferenciada ou semelhante, de institutos jurídicos, normas e conceitos nos vários ordenamentos jurídicos, com o fito de esclarecer o significado a atribuir a determinados enunciados linguísticos utilizados na formulação de normas jurídicas. Modernamente, tem-se elevado a interpretação comparativa à condição de quinto método de interpretação.

[514] Segundo o mesmo método de interpretação, o jurídico, não é admissível se interpretar além do que diz o texto constitucional ou, muito menos, ir contra seu teor literal (CANOTILHO, 2000, p. 1211).

art. 225, §3º, todos da CF) sejam providos de condições para atuar com eficiência[515] nesses novos tempos.

Portanto, admitir que a inviolabilidade de alguma forma comunicativa pudesse servir de salvaguarda para o cometimento de crimes violaria, segundo precedente do Tribunal Constitucional Alemão[516] citado por Alexy (2011), a própria noção de unidade da Constituição[517]. Diz o precedente germânico que somente direitos fundamentais de terceiros e outros valores jurídicos de hierarquia constitucional estão em condições de, excepcionalmente e com a devida consideração à unidade da Constituição e à ordem de valores por ela protegida, restringir, em relações individualizadas, direitos fundamentais irrestringíveis.

No Brasil, em precedente de 1984, o Supremo Tribunal Federal admitiu a fiscalização do conteúdo da correspondência de presos, com base em dispositivo infraconstitucional que dispõe que ato motivado do diretor do presídio poderá suspender ou restringir o direito do preso de manter contato com o mundo exterior por meio de correspondência escrita (art. 41, XV e §único, da Lei 7.210/84). Na fundamentação, afirmou a Corte que a inviolabilidade do sigilo epistolar não poderia constituir instrumento de salvaguarda de práticas ilícitas[518].

É inegavelmente questionável a correção de tal solução, vez que contraria frontalmente um mandamento constitucional direto e sem margem para dúvidas gramaticais.

No entanto, veja-se que o mesmo precedente alemão afirma que os conflitos que surgem nesse âmbito só podem ser resolvidos se se examina qual dispositivo constitucional tem maior peso para a questão concreta a ser decidida, de modo que a norma mais fraca só pode ser deixada em segundo plano na medida do necessário ponto de vista lógico e sistemático, devendo-se, em qualquer caso, respeitar o seu conteúdo axiológico fundamental. A questão, portanto, residiria em saber se há alternativas a esse tipo de fórmula, ao mesmo tempo aceitáveis e livres de sopesamento[519].

Acrescenta-se que, como visto anteriormente[520], o âmbito de proteção de um direito fundamental não pode ser fixado em regras gerais, sendo necessário um procedimento para cada direito, exigindo-se uma interpretação sistemática que terá que considerar outros direitos a serem com ele confrontados.

Como o precedente envolvendo a fiscalização de correspondência epistolar dos presos não é objeto do presente trabalho, cabe aqui analisar apenas as duas últimas formas

---

[515] Sobre os conceitos de eficiência e garantismo, ver item 3.2.
[516] *BVerfGE*, 28, 243 (26).
[517] ALEXY, 2011, p. 124/125.
[518] BRASIL. Supremo Tribunal Federal. HC 70.814, rel. min. Celso de Mello, j. 01.03.1994, DJ 24.06.1994.
[519] ALEXY, 2011, p. 125.
[520] Ver item 6.1.2, *supra*.

comunicativas constantes da norma do inciso XII do artigo 5º da Constituição de 1988, quais sejam, as comunicações de dados e telefônicas.

Quanto a elas, observando-se a inadmissibilidade de se adotar qualquer linha interpretativa que exceda ou contrarie o teor de um mandamento constitucional, própria do método jurídico, e considerando, também, a já mencionada ambiguidade linguística existente naquele dispositivo, pode-se dizer que não haveria nenhuma – digamos – vedação constitucional explícita a que se admita a possibilidade de excepcionar a inviolabilidade do sigilo dessas formas comunicativas.

Quanto à análise do cabimento de interceptação de comunicações em situações concretas, o que é prescrito pela metódica jurídica normativo-estruturante, isso será tarefa da legislação infraconstitucional, cuja correção e limites serão analisados no item 4.3, *infra*.

Neste ponto do presente trabalho, de análise das exceções constitucionalmente admitidas à inviolabilidade do sigilo daquelas duas últimas modalidades comunicativas referidas no inciso XII, cabe apenas concluir pelo afastamento da ideia de uma inviolabilidade absoluta.

4.2 Classificação probatória

Há duas concepções de prova atípica: a restritiva e a ampliativa. Segundo a primeira, prova atípica é aquela não nominada em lei, ou seja, que não conta com nenhuma previsão ou menção na legislação. Já na concepção ampliativa, prova atípica é a que não conta com nenhuma menção ou nominação em lei, mas também a que é nominada na lei, porém sem previsão de procedimento probatório[521].

Nesse sentido, as interceptações telefônicas e telemáticas no Brasil passaram por três fases: (1) até a promulgação da CF de 1988, eram, sem dúvida, 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[522].

---

[521] DEZEM, Guilherme Madeira. **Da prova penal**: tipo processual, provas típicas e atípicas (atualizado de acordo com as Leis 11.689, 11.690 e 11.719/08), Campinas: Millennium Editora, 2008, p. 155.

[522] A legalidade do meio de obtenção de prova é pressuposto do princípio da proporcionalidade (FERNANDES, 2010, p. 52).

Considerando que se está tratando da interceptação telemática, que é meio de obtenção de prova[523] usado na fase pré-processual, na qual ao investigado não são concedidas as garantias que incidem sobre os meios de prova, próprios da fase judicial, é inaplicável a regra geral do Código de Processo Civil (CPC), segundo a qual são admissíveis "todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código..." (art. 332, CPC), ou seja, não se pode abrir mão da tipicidade probatória para a admissibilidade da interceptação telemática.

Foi este mesmo fundamento, qual seja, a falta de previsão legal das hipóteses de cabimento da interceptação, que levou o Supremo Tribunal Federal (STF) a consolidar a inadmissibilidade das interceptações de comunicações promovidas entre 1988 e 1996, tratando o seu produto como prova ilícita.

No *leading case* HC 69912/RS, o ministro relator invocou as palavras de Ada Pellegrini Grinover no sentido de que, "enquanto não vier a lei a estabelecer as hipóteses e a forma em que as interceptações poderão ser permitidas, não haverá, por enquanto, como ordená-las, pois o Código de Telecomunicações nada especifica, não suprimindo a ausência de lei específica". Acrescentou que entendimento contrário "esvaziaria por completo a garantia constitucional, na medida em que a faria vulnerável a toda forma de arbítrio judicial"[524].

Na renovação do julgamento acima, porquanto no primeiro verificou-se a participação de ministro impedido, afirmou-se que o inciso XII do artigo 5º não se reveste de densidade normativa suficiente, impondo e reclamando um processo de integração normativa de que derivasse a lei que era exigida pela própria Constituição[525].

Dois anos depois, no julgamento do HC 72588/PB, a Corte ratificou seu entendimento, fazendo observar que "não ha[via] que se argumentar com o Código Brasileiro de Telecomunicações, cujo artigo 57, inciso II, alínea '*a*', não foi recepcionado pela Carta Política atual, em face da natureza do conceito emitido pelo inciso XII, do artigo 5º, a exigir, *numerus clausus*, definição das 'hipóteses e formas' para a outorga da autorização judicial"[526].

---

[523] Ver item 4.2, *supra*.

[524] BRASIL. Supremo Tribunal Federal. HC 69.912/RS, rel. min. Sepúlveda Pertence, red. p/ acórdão min. Carlos Veloso, Pleno, j. 30.06.1993, DJ 26.11.1993.

[525] BRASIL. Supremo Tribunal Federal. HC 69.912/RS-segundo julgamento, Pleno, rel. min. Sepúlveda Pertence, j. 16.12.1993, DJ 25.03.1994.

[526] BRASIL. Supremo Tribunal Federal. HC 72.588/PB, rel. min. Maurício Corrêa, Pleno, j. 08.11.1995, DJ 04.08.2000. No mesmo sentido, BRASIL. Supremo Tribunal Federal. HC 74116/SP, rel. min. Néri da Silveira, rel. p/ acórdão min. Maurício Corrêa, 2ª T, j. 05.11.1996, DJ 14.03.1997.

E a sanção processual adotada pela Corte nesses e em tantos outros precedentes foi a inadmissibilidade do material interceptado, tal qual impõe o artigo 5º, inciso LVI da Constituição Federal[527].

A interceptação das comunicações telemáticas no Brasil é, portanto, meio de obtenção de prova típico.

4.3 Pressupostos

As exigências da Lei 9.296/96 para que seja concedida autorização judicial para interceptar as comunicações de um indivíduo, sejam as telefônicas, sejam as de fluxo de comunicações em sistemas de informática e telemática (art. 1º, § único) são, cumulativamente[528], a existência de indícios razoáveis da autoria ou participação em infração penal (art. 2º, I), que a esta infração seja cominada pena de reclusão (art. 2º, III) e a impossibilidade de que a prova seja feita por outros meios disponíveis (art. 2º, II).

As prescrições legais acima, no entanto, foram concebidas pelo legislador em redação negativa, que lista as hipóteses nas quais *não* será admitida a interceptação (art. 2º, *caput*), o que foi criticado por Vicente Greco Filho (2005), por entender que a redação poderia sugerir que a interceptação fosse a regra e o sigilo a exceção, e que melhor teria sido que a lei houvesse indicado, taxativamente, os casos que admitissem a medida[529].

Por ser providência cautelar, exige-se a presença de *fumus boni iuris*, expresso na probabilidade 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[530].

Verifica-se, inclusive, que a redação legal não se contentou com a mera possibilidade de autoria ou participação, tendo exigido, com o emprego da expressão "razoáveis", uma autoria ou participação que seja provável[531].

---

[527] "Não havendo ato legislativo que discipline o mecanismo do inciso XII, do artigo 5º, da CF, é de aplicar-se o comando constitucional do inciso LVI, deste mesmo artigo, que prescreve serem 'inadmissíveis, no processo, as provas obtidas por meios ilícitos'" (BRASIL. Supremo Tribunal Federal. HC 72.588/PB, rel. min. Maurício Corrêa, Pleno, j. 08.11.1995, DJ 04.08.2000).
[528] GOMES; CERVINI, 1997, p. 178.
[529] GRECO FILHO, 1996, p. 13/14.
[530] FERNANDES, 2010, 96/97.
[531] GOMES; CERVINI, 1997, p. 178.

Enquanto no ordenamento brasileiro, portanto, há que se aferir a presença de indícios razoáveis da autoria ou participação, nos Estados Unidos da América, fala-se em *probable cause* (*probable cause* de que um indivíduo esteja cometendo, tenha cometido ou esteja em vias de cometer determinado crime; e *probable cause* de que a interceptação requerida irá captar comunicações relativas àquele crime)[532].

A nosso ver, não há diferença relevante a se destacar entre essas duas formas, a americana e a brasileira, com as quais um e outro ordenamento prescreveram a exigência de um juízo de probabilidade, verossimilhança ou plausibilidade para se autorizar a interceptação de comunicações.

Aliás, mais do que não vislumbrar distinção relevante, parece-nos que nesse campo, do estudo dos níveis de certeza judicial, da apuração dos significados de expressões legais como *indícios suficientes* ou *indícios razoáveis*[533], e por mais que existam esforços doutrinários para sistematizá-lo ou para criar espécies de microssistemas capazes de uniformizar seu tratamento e interpretação[534], a escolha do caminho a seguir no caso concreto acabará sempre entregue nas mãos da mais irracional, incontrolável e imprevisível discricionariedade humana do julgador, suscetível das mais peculiares e desconhecidas influências, que poderão decorrer da história de vida e da personalíssima percepção mental de cada um.

Nas palavras de Calamandrei, no momento final do julgamento, intervém na consciência do juiz uma espécie de iluminação irracional, um autêntico ato de fé, que transforma a probabilidade em certeza[535].

Expressões como probabilidade, verossimilhança ou plausibilidade do direito invocado constituem-se, na verdade, em expressões sem conteúdo definido, o que possibilita

---

[532] Tratamos do conceito de *probable cause* nos itens 3.1.4 e 3.1.5.

[533] MARQUES, José Frederico. **Elementos de direito processual penal**. v. IV. Rio de Janeiro: Forense, 1965, p. 115; BARROS, Romeu Pires de Campos. **Processo penal cautelar**. Rio de Janeiro: Forense, 1982, p. 194; TOURINHO FILHO, Fernando da Costa. **Processo penal**. v. 3. 21ª ed. São Paulo: Saraiva, 1999, p. 90).

[534] Chiovenda fala em possibilidade do direito (CHIOVENDA. Giuseppe. **Principii di diritto processuale civile**. 3ª ed. Napoli: Jovene, 1965, p. 227). Calamandrei e Liebman se referem a um *giudizio di probabilità* (CALAMANDREI, Piero. **Introduzione allo studio sistematico dei provvedimenti cautelari**. Opere giuridiche. v. IX. Napoli: Morano, 1983, p. 201; LIEBMAN, Enrico Tullio. **Unità del procedimento cautelare**. Problemi del processo civile. Napoli: Morano, 1962, p. 108). José Roberto dos Santos Bedaque fala da probabilidade de que o direito exista (BEDAQUE, José Roberto dos Santos. Tutela cautelar e tutela antecipada: tutelas sumárias e de urgência: tentativa de sistematização. São Paulo: Malheiros, 1998, p. 174). Ovídio Batista fala em plausibilidade do direito invocado (SILVA, Ovídio A. Batista da. **As ações cautelares e o novo processo civil**. 3ª ed. Rio de Janeiro: Forense, 1980, p. 51).

[535] CALAMANDREI, Piero. Verità e verosimiglianza nel processo civile. In: **Rivista di Diritto Processuale**, p. 164/192, Milano: Giuffrè, 1955, p. 166.

ao juiz, em cada caso concreto, maior liberdade para identificar a presença do requisito necessário à concessão de uma cautelar[536].

Seja como for, no que se refere às exigências para interceptação de comunicações, tais indícios de autoria ou participação precisam ser prévios[537], não se podendo autorizar uma interceptação com base em meras conjecturas ou suspeitas, já que não se admite a chamada interceptação de prospecção para se descobrir se uma pessoa estaria ou não envolvida em algum possível crime[538].

Já a exigência do artigo 2º, II, quanto a haver ou não *outros meios disponíveis* pelos quais a prova possa ser feita, tais meios não devem ser interpretados como aqueles a que materialmente a autoridade policial tenha à sua disposição, mas sim os meios legais-processuais, sob pena de que simples alegação da polícia de que não possui outros meios bastasse para se obter uma autorização para interceptação[539].

Ao comentar a dificuldade que tende a recair sobre o magistrado incumbido de analisar se existem ou não outros meios disponíveis, Antonio Scarance Fernandes observa que o convencimento do juiz deverá ser extraído com base nos meios que eram ou podiam ser de seu conhecimento no momento da decisão, de modo que não se deve taxar de ilegítima a autorização judicial quando, depois, venha a se demonstrar a existência de outros meios, antes desconhecidos ou descobertos posteriormente, exceto quando se evidenciar que a autoridade policial, agindo de má-fé, escondeu do juiz meios suficientes para obter a prova pretendida[540-541].

E tal pressuposto, do artigo 2º, II, ao que nos parece, se liga intimamente ao do artigo 4º, que exige também que a medida se mostre necessária à apuração da infração penal. São estas, a nosso ver, enfim, as maiores dificuldades que se apresentam ao juiz, a de verificar se a medida é necessária e se, além disso, há ou não outros meios disponíveis, menos gravosos, para se fazer a prova.

Como se trata de conceitos passíveis das mais díspares interpretações, importa observar que a restrição de um direito fundamental não deve ser balizada por comodismo ou

---

[536] BEDAQUE, José Roberto dos Santos. **Tutela cautelar e tutela antecipada**: tutelas sumárias e de urgência (tentativa de sistematização). São Paulo: Malheiros, 1998, p. 175.
[537] FERNANDES, 2010, p. 96.
[538] GOMES; CERVINI, 1997, p. 179/180.
[539] STRECK, 2001, p. 52/53.
[540] FERNANDES, 2010 p. 97.
[541] Também para Vicente Greco Filho (1996, p. 17/18), se a autoridade policial obtém autorização judicial para interceptação mediante a ocultação de outros meios de prova disponíveis, ou se se verifica que houve desinteresse de sua parte em adotar medida menos gravosa, a prova estará gravada de ilicitude.

mesmo por uma busca de máxima eficiência da persecução penal[542] e que a interpretação do termo *necessária* deve ser sistemática e restritiva, de modo a evitar a chamada generosidade nas autorizações judiciais[543] de interceptação.

A exigência de que a medida seja necessária, inscrita no artigo 4º, expressa a observância ao princípio da proporcionalidade, precisamente em seu subprincípio necessidade ou menor ingerência possível[544], orientando o intérprete a optar pela intervenção mínima, pela alternativa menos gravosa, o que obrigaria os órgãos do Estado a comparar as medidas restritivas aplicáveis que sejam suficientemente aptas à satisfação do fim perseguido e a eleger, finalmente, a que seja menos lesiva para os direitos dos cidadãos[545].

Aliás, quanto a esse dever de comparar a medida de interceptação de comunicações com outras menos gravosas que também possam satisfazer a demanda probatória, a lei inglesa, retratada no item 3.2.3, andou bem ao dispor que, ao autorizar a interceptação, o Secretário de Estado deverá verificar se ela é proporcional ao fim a que se destina, devendo, ainda, em tal verificação, certificar-se de que o resultado pretendido não possa ser razoavelmente obtido por outros meios.

Mas ainda melhor andou o legislador norte-americano, que conseguiu inserir em sua legislação uma imposição que nos parece bastante eficiente no sentido de efetivamente assegurar que os personagens envolvidos na implementação da interceptação – entenda-se policial que a requer e juiz que a autoriza (ou que aprova interceptação pretérita) – farão uma comparação com outras medidas investigatórias, menos gravosas, que possam realizar os mesmos objetivos probatórios pretendidos. Dispôs a lei daquele país que, tanto no requerimento de autorização, quanto na decisão que a concede, deverá constar a descrição de procedimentos investigatórios normais que tenham sido tentados e falharam ou a exposição das razões pelas quais tais procedimentos não foram tentados, já que, por sua natureza, seriam incapazes de atingir o objetivo probatório pretendido ou que seriam perigosos demais.

Os métodos inglês e norte-americano, mas em especial o último, apresentam-se como sábias opções legislativas, capazes de implementar, mais eficientemente, a observância ao princípio da proporcionalidade, especificamente quanto a seu subprincípio da exigibilidade material, que exige que o meio empregado seja o mais comedido possível quanto à limitação do direito fundamental[546].

---

[542] BADARÓ, 2010, p. 493.
[543] STRECK, 2001, p. 54.
[544] Tratamos do princípio da proporcionalidade e de seus subprincípios no item 1.4.
[545] CERVINI; GOMES, 1997, p. 182/183.
[546] Sobre o subprincípio da exigibilidade material, ver item 1.4.

Como não vislumbramos nenhum óbice a que se importem os dois aspectos das realidades inglesa e norte-americana para a brasileira, afirmamos que a inserção de dispositivo análogo nesta última teria contribuído para a busca do equilíbrio, descrito por Scarance Fernandes[547], entre um hipergarantismo e uma repressão a todo custo, aproximando, portanto, o intérprete e operador do direito brasileiro da meta de um ponto médio existente entre a proteção à liberdade e a segurança da sociedade.

Na esteira de tudo que se expôs acima, entendemos, também, que o Estado não poderá lançar mão da interceptação de comunicações como primeiro ato investigatório[548].

Quanto à exigência objetiva do artigo 2º, III, qual seja, a de que o crime a ser investigado seja punido com pena de reclusão, muitas foram as críticas da doutrina quanto a se tratar, por um lado, de exagero a permissão a que qualquer crime punido com reclusão admita interceptação[549] e, por outro, de restrição demasiada a impossibilidade absoluta de que a medida seja empregada na investigação de crimes punidos com detenção[550].

Nesse ponto, o Projeto de Código de Processo Penal contém avanços, mas também retrocessos. Seu artigo 247, mantendo a mesma redação negativa criticada na lei atual, permite, por um lado, a interceptação para investigar crimes de menor potencial ofensivo que tenham sido praticados por telefone, mas, por outro, amplia a admissibilidade da medida para todo e qualquer crime[551-552].

---

[547] Ver item 1.4.

[548] Entendendo diversamente, Gomes e Cervini (1997, p. 180) afirmam que a interceptação pode ser o primeiro ato de investigação criminal desde que já existam indícios razoáveis de autoria ou participação em uma infração penal.

[549] FERNANDES, 2010, 97/98; GRECO FILHO, 1996, p. 14/16; e GOMES; CERVINI, 1997, p. 185/186.

[550] Scarance Fernandes menciona o jogo do bicho e os crimes de ameaça ou injúria cometidos por telefone como exemplos de crimes punidos com detenção que deveriam admitir interceptação (SCARANCE, 2010, 97/98). Lênio Streck afirma que deveriam estar no rol alguns crimes punidos com detenção, como ameaça cometida por meio telefônico ou contravenções que, como o jogo do bicho, seriam mais fortemente recriminadas pela sociedade (STRECK, 2001, p. 56); Gomes e Cervini mencionam também a ameaça e o crime contra a honra cometido por telefone como exemplos de crimes punido com detenção que deveriam admitir a interceptação (GOMES; CERVINI, 1997, p. 185/186).

[551] Art. 247. A interceptação de comunicações telefônicas não será admitida na investigação criminal ou instrução processual de crimes de menor potencial ofensivo, assim definidos no art. 288, salvo quando a conduta delituosa for realizada exclusivamente por meio dessa modalidade de comunicação (Parecer nº 1.636, de 2010, estabelecendo a redação final do Projeto de Lei do Senado nº 156, de 2009. Disponível em: <http://www.senado.gov.br/atividade/materia/getPDF.asp?t=85509&tp=1>. Acesso em: 22 dez. 2013).

[552] Na manifestação do IBDP acerca do Projeto, sugere-se redação com o seguinte rol de crimes: Art. 241. A quebra do sigilo das comunicações telefônicas de qualquer natureza é admissível para fins de investigação criminal e instrução processual penal relativas aos seguintes crimes: I – tráfico de substâncias entorpecentes e drogas afins; II – tráfico de seres humanos e subtração de incapazes; III – tráfico de armas, munições e explosivos; IV – tráfico de espécimes da fauna silvestre; V – corrupção de menores; VI – lavagem de dinheiro; VII – contra o sistema financeiro nacional; VIII- contra a ordem econômica e tributária; IX – contra a administração pública**,** desde que punidos com pena de reclusão; X – falsificação de moeda ou a ela assimilados; XI – roubo, latrocínio, extorsão simples, extorsão mediante sequestro, sequestro e cárcere privado; XII – homicídio doloso; XIII – ameaça e crimes contra a honra, quando cometidos por meio de comunicação telefônica; XIV – decorrente de ações praticadas por organização criminosa; XV – decorrente de ações de

Lenio Streck (2001) sustenta que os crimes a admitir a medida deveriam ser aqueles indicados na Constituição como de extrema gravidade, a exemplo dos inafiançáveis e dos cometidos contra o meio ambiente e contra a humanidade[553].

Para Scarance Fernandes (2010)[554], diante da possibilidade de que a medida seja útil tanto em crimes mais graves, quanto em crimes menos graves, melhor teria sido se a lei determinasse quais crimes comportam a medida, como fez o Projeto Miro Teixeira[555].

Já Vicente Greco Filho (2005)[556] entende que não seria possível estabelecer previamente quais os crimes dignos de interceptação, mas advoga, para além da mera consideração da pena cominada em abstrato, a ponderação quanto aos bens jurídicos envolvidos por meio do princípio da proporcionalidade.

A nosso ver, retirar da lei toda e qualquer restrição prévia acerca dos crimes que admitem a medida, deixando totalmente a critério do juiz a avaliação dos bens jurídicos envolvidos, implicaria em ampliar demais sua margem de discricionariedade. Nesse sentido, por mais que a lei, a exemplo do que se fez na Inglaterra, impusesse textualmente ao magistrado o dever de decidir à luz do princípio da proporcionalidade[557], a legislação brasileira estaria a infringir o subprincípio da exigibilidade espacial, que exige limitações ao âmbito da intervenção que o Estado promoverá sobre os direitos do indivíduo[558].

É claro que se poderia argumentar que o subprincípio da exigibilidade espacial estaria atendido na medida em que a limitação do âmbito de intervenção terá saído da lei, transferindo-se, todavia, ao juiz, mas tal raciocínio importaria em verdadeira involução e retrocesso nos padrões de proteção aos direitos humanos já alcançados e consolidados pelas cortes internacionais de direitos humanos.

Isto porque, conforme abordado no item 1.3, *supra*, tanto a interpretação dada ao artigo 11 da Convenção Americana de Direitos Humanos pela Corte IDH, quanto a que o TEDH deu ao artigo 8º da Convenção Europeia são no sentido de exigir que medidas de interceptação das comunicações estejam, não só previstas em lei, mas que a lei indique, com

---

terrorismo. (Instituto Brasilero de Direito Processual (IBDP). Propostas de emendas ao Projeto de Lei de Código de Processo Penal. Substitutivo CCJ do Senado (Disponível em: <http://www.direitoprocessual.org.br/download.php?f=9546b22fe462eb3d2116f6ff5b62a312>. Acesso em: 05 jan. 2014).

[553] STRECK, 2001, p. 56.

[554] FERNANDES, 2010, p. 97.

[555] BRASIL. Câmara dos Deputados. PL nº 3.514/1989. Autor Deputado Miro Teixeira. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=55F3499F5ADD4FBB2DCEB356B0FF8DC7.node2?codteor=1155030&filename=Avulso+-PL+3514/1989 >. Acesso em: 22 dez. 2013.

[556] GRECO FILHO, 1996, p. 14/16.

[557] No caso da Inglaterra a imposição não foi dirigida propriamente a o magistrado, mas ao Secretário de Estado, autoridade com poder para conceder autorização para fins de interceptação de comunicações (Ver item 3.2.3).

[558] Sobre o subprincípio da exigibilidade espacial, ver itam 1.4.

clareza e precisão, as condições e a forma pelas quais os poderes públicos estão autorizados a exercer sua discricionariedade, dando ao indivíduo, portanto, uma previsibilidade das suas consequências. Vale lembrar, nesse sentido, que o TEDH reconheceu violação à Convenção Europeia no caso Calogero Diana vs. Itália[559] porque a lei interna teria deixado às autoridades uma margem excessiva de discricionariedade, bem como no caso Kopp vs. Suíça[560] porque a lei suíça não indicava, com clareza, as condições e a forma pela qual as autoridades deveriam exercer sua discricionariedade sobre a matéria.

Entendemos, nesse sentido, que o primeiro a seguir o subprincípio da exigibilidade espacial, positivando o referido subprincípio, deverá ser, na hipótese, o legislador, que deverá estabelecer um rol dos crimes que admitam a interceptação de comunicações.

Para conceber o referido rol, deve o legislador se basear, não só no critério da gravidade do crime – e aqui haver-se-ia que incluir, evidentemente, todos aqueles que sejam objeto de mandamento constitucional de criminalização[561] –, mas também no *modus operandi*, de forma que, assim como entenderam Scarance Fernandes, Luiz Flavio Gomes e Lenio Streck em relação à ameaça e à injúria cometidas por telefone, entendemos que deveriam constar do rol todos aqueles crimes ou contravenções que, embora de menor potencial ofensivo, fossem praticados através de e-mail, *Facebook* ou outro veículo de comunicação baseado em internet ou comunicação digital.

No entanto, no que se refere à previsão dos crimes que admitem interceptação, pode-se dizer que a legislação brasileira atual, ainda que merecedora das críticas acima, afastou-se menos dos parâmetros de eficiência e garantismo do que a dos Estados Unidos, pois esta admitiu a medida para todo e qualquer crime federal[562].

4.4 Prazo

Para se falar em prazo de duração da interceptação, um dado essencial a ser considerado preliminarmente será, naturalmente, a data de início da medida, algo que, apesar

[559] Precedente analisado no item 1.3.
[560] Precedente analisado no item 1.3.
[561] Pode-se citar a discriminação atentatória dos direitos e liberdades fundamentais, o racismo, a tortura, o tráfico ilícito de entorpecentes e drogas afins, o terrorismo e os definidos como crimes hediondos, a ação de grupos armados, civis ou militares, contra a ordem constitucional e o Estado Democrático (art. 5º, XLI, XLII, XLIII e XLIV), a retenção dolosa de salário (art. 7, X), as condutas e atividades consideradas lesivas ao meio ambiente (art. 225, §3º) e o abuso, a violência e a exploração sexual da criança e do adolescente (art. 227, §4º).
[562] Ver item 3.1.5.

de parecer simples, a prática já mostrou não ser. A só existência de precedentes jurisprudenciais recorrentes sobre o tema já demonstra a existência de dúvidas e divergências em torno dele[563].

Mais complexo do que definir um conceito de data inicial – até porque pode-se classificar até de intuitiva a conclusão de que se deve considerar a data de início aquela em que a interceptação efetivamente começou, e não a data da decisão autorizativa – será a verificação da data em que a polícia verdadeiramente começou a captar as comunicações do investigado, sem que tal informação advenha de declaração unilateral da própria polícia. Isto porque, atualmente, a única forma de se verificar isto nos autos é através das decisões autorizativas e do próprio material captado, a partir dos quais os sujeitos processuais terão de deduzir os momentos de início de cada período autorizado de interceptação e verificar o respeito aos prazos. Noutras palavras, será o órgão de investigação, ao inserir nos autos as comunicações captadas, quem dará as cartas quanto à indicação do que a defesa poderá vir a presumir ser a provável data de início da medida. Não haverá meios de a defesa saber, por exemplo, se, por força de qualquer interesse ou conveniência escusa, a polícia cuidou de excluir os dois primeiros dias da quinzena, fosse para incluir mais dois ao final que não

[563] "DILIGÊNCIAS COMPLEMENTARES REQUERIDAS NA FASE DO ART. 499 DO CPP (PEDIDO DE INFORMAÇÕES À RECEITA FEDERAL ... E DE ESPECIFICAÇÃO DAS DATAS DE INÍCIO E TÉRMINO DAS INTERCEPTAÇÕES TELEFÔNICAS REALIZADAS). PEDIDOS INDEFERIDOS PELO JUÍZO PROCESSANTE. ALEGAÇÃO DE CERCEAMENTO DE DEFESA. INDEFERIMENTO DEVIDAMENTE FUNDAMENTADO. IMPERTINENTE A COLHEITA DE ESCLARECIMENTOS QUE NÃO DIZEM RESPEITO À CONDUTA IMPUTADA AO RECORRENTE" (BRASIL. Superior Tribunal de Justiça. RMS 28284/RJ, rel. Napoleão Nunes Maia Filho, 5ª T., j. 04.12.2009, DJe 22.02.2010); "1. A Lei n.º 9.296/96, que regula as medidas constritivas de captação de comunicações via telefone, não estipula prazo para o início do cumprimento da ordem judicial. 2. Conquanto não se possa ter delonga injustificada para o começo efetivo da interceptação telefônica, cada caso deve ser analisado sempre à luz do princípio da proporcionalidade e, na hipótese em exame, a greve da Polícia Federal consiste em evento idôneo para a demora no início da interceptação, não se violando, pois, o dado princípio. 3. In casu, a letargia de 3 (três) meses para a execução da decisão deveu-se unicamente a ocorrência de greve policial, sendo que, após o início efetivo da medida, data tida como marco inicial para a contagem do prazo, foi observado o lapso quinzenal previsto em lei, inexistindo qualquer ilegalidade na prova obtida. 4. Ordem denegada" (BRASIL. Superior Tribunal de Justiça. HC 113477/DF, rel. min. Maria Thereza de Assis Moura, 6ª T., j. 20.03.2012, DJe 16.04.2012); "TERMO INICIAL A PARTIR DA IMPLEMENTAÇÃO PELA OPERADORA DE TELEFONIA. ... 2. Em relação às interceptações telefônicas, o prazo de 15 (quinze) dias, previsto na Lei n. 9.296/96, é contado a partir da efetivação da medida constritiva, ou seja, do dia em que se iniciou a escuta telefônica e não da data da decisão judicial (HC n. 135.771/PE, Ministro Og Fernandes, DJe 24/8/2011). 3. No caso, o termo inicial efetivo da medida constritiva é 29/9/2009, e os dias 7, 8 e 9/10/2009, incluídos na contagem do lapso de 15 dias, estão no prazo legal" (BRASIL. Superior Tribunal de Justiça. HC 212643/PE, rel. min. Sebastião Reis Júnior, 6ª T., j. 06.03/2012, DJe 26.03.2012); "1. Embora a decisão que autorizou a diligência pelo prazo de quinze dias tenha sido proferida no dia 14 de agosto de 2008, a interceptação telefônica se iniciou no dia seguinte, logo, a medida ainda estaria autorizada no dia 30 do mesmo mês" (BRASIL. Superior Tribunal de Justiça. HC 144378/DF, rel. min. Laurita Vaz, 5ª T., j. 22.11.2011, DJe 02.12.2011).

estivessem contemplados por uma autorização, fosse porque surgiram indícios da prática de crime por pessoa de persecução politicamente desinteressante[564].

O problema se deve ao fato de a legislação brasileira não prever um *dies a quo* para a contagem do prazo e, muito mais do que isso, de não estabelecer mecanismos para registrar nos autos os períodos em que as comunicações efetivamente foram fornecidas ou desviadas pelo provedor de e-mails ou prestador de serviços de comunicações ao órgão de investigação.

Quanto a esse aspecto, a legislação norte-americana trouxe dispositivo prevendo que o prazo começa a ser contado na manhã do dia em que a interceptação começa a ser executada ou, senão, no décimo dia após a expedição da autorização[565].

No Brasil, a redação proposta no §1º do artigo 252 do Projeto de Código de Processo Penal estabelece para os prestadores de serviços de comunicações o dever de comunicar ao juiz, por escrito, a data de início da interceptação[566], o que poria fim à celeuma[567].

Pode-se dizer, portanto, que a legislação dos Estados Unidos contém, nesse ponto, aspecto mais eficiente do que a brasileira, no sentido de, ainda que com critérios objetivos que levam em conta momentos presumidos do início da medida, permitir uma melhor fiscalização defensiva da obediência aos prazos, evitando-se a captação e utilização probatória de comunicação captada ilicitamente.

A redação do Projeto de CPP brasileiro seria, no entanto, capaz de atender ainda melhor aos critérios de eficiência, eficácia e efetividade, na medida em que, ao estabelecer uma comunicação direta entre a prestadora de serviços de comunicação e o juiz, de modo a fazer registrar nos autos o momento exato do início da interceptação, cumpriria a finalidade de permitir aos sujeitos processuais, especialmente ao réu, o exercício de seu direito de

---

[564] No sentido de mostrar a incapacidade que a defesa terá de demonstrar a efetiva data de início da interceptação, mostra-se sintomática a passagem do voto do ministro Gilson Dipp, no julgamento do RHC 13274/RS: "o prazo legal refere-se à execução da diligência e não à data da decisão do Juiz. Ou seja, o dia em que se iniciou a escuta telefônica propriamente dita é que deve ser tomado como marco para a contagem do prazo. Assim, como a execução da diligência dependia da implantação do terminal pela companhia telefônica, dificilmente essa providência teria sido tomada no mesmo dia da decisão que determinou a expedição de alvará de escuta (fl. 106). E, se o foi, não há como saber à vista dos documentos que instruíram a impetração" (BRASIL. Superior Tribunal de Justiça. RHC 13274/RS, rel. min. Gilson Dipp, 5ª T., j. 19.08.2003, DJ 29.09.2003).

[565] Ver item 3.1.5.

[566] Art. 252. ... § 1º O prazo correrá de forma contínua e ininterrupta e será contado a partir da data do início da interceptação, devendo a prestadora responsável pelo serviço comunicar imediatamente esse fato ao juiz, por escrito (Parecer nº 1.636, de 2010, estabelecendo a redação final do Projeto de Lei do Senado nº 156, de 2009. Disponível em: <http://www.senado.gov.br/atividade/materia/getPDF.asp?t=85509&tp=1>. Acesso em: 25 dez. 2013).

[567] Na Espanha, há previsão semelhante, embora não tão eficiente, no sentido de que o prestador de serviço de comunicações incumbido de viabilizar a interceptação deverá notificar o investigador do momento em que o mecanismo de interceptação for ativado (Ver item 3.3.2, *supra*). Afirmamos que não é tão eficiente porque a notificação imposta deve ser dirigida ao investigador, e não ao juiz, como na redação do Projeto de CPP brasileiro.

defesa[568], que, neste ponto, dependerá da aferição, ainda que *post facto*, da regularidade da interceptação.

Dito isto sobre o termo inicial da contagem do prazo de duração da interceptação, passa-se a tratar do prazo propriamente dito, de sua extensão.

O artigo 5º da Lei 9.296/96 estabelece que a interceptação não poderá exceder o prazo de quinze dias, renovável por igual tempo, uma vez comprovada a indispensabilidade do meio de prova.

Entende-se, majoritariamente, no entanto, que não há limite temporal para o número de prorrogações. Nesse sentido, Vicente Greco Filho (1996) entende que a lei não limitou o número de prorrogações possíveis, podendo haver quantas prorrogações sejam necessárias à investigação, mesmo porque 30 dias pode ser um prazo muito exíguo[569].

Já Gomes e Cervini (1997) reconhecem que o limite temporal faz parte da proporcionalidade em abstrato, da qual se encarregou o legislador, já que toda medida restritiva de direito deve ter limite, mas sustentam, igualmente, que não haveria limite de quantas vezes pode ser renovada a interceptação, já que a lei não especificaria isso, bastando que a medida continue sendo indispensável e necessária[570].

Para Guilherme de Souza Nucci (2011), da mesma forma, não haveria o menor sentido em se impor uma limitação em dias, "sob pena de frustrar a busca da verdade real, além de se frear a atividade persecutória lícita por uma mera questão temporal"[571]. Disse, ainda, que a interceptação poderá perdurar enquanto for útil à colheita da prova[572].

Nos tribunais, durou pouco a linha inaugurada pela Sexta Turma do STJ[573], segundo a qual se impunha o limite de quinze dias, renováveis, uma vez, por igual período. O entendimento logo foi substituído pela jurisprudência atual, que admite quantas prorrogações forem necessárias à investigação[574], havendo uma resistência minoritária, de uns poucos magistrados, no sentido de manter o entendimento anterior[575].

---

[568] A verificação abstrata ou concreta da eficiência, eficácia ou efetividade de algum aspecto processual, depende da verificação de sua finalidade, que, no que se refere ao processo, seria a de permitir a todos os seus sujeitos o exercício de suas faculdades, de seus direitos, de suas garantias, de seus poderes (Ver item 1.4).

[569] GRECO FILHO, 1996, p. 31.

[570] GOMES; CERVINI, 1997, p. 218/219.

[571] NUCCI, Guilherme de Souza. **Código de Processo Penal comentado**. 10ª ed. São Paulo: Revista do Tribunais, 2011, p. 378.

[572] Id., **Leis penais eprocessuais penais comentadas**. 5ª ed. São Paulo: Revista dos Tribunais, 2010. p. 802.

[573] BRASIL. Superior Tribunal de Justiça. HC 76686/PR, rel. min. Nilson Naves, 6ª T., j. 09.09.2008, DJe 10.11.2008.

[574] "É possível a prorrogação do prazo de autorização para a interceptação telefônica, mesmo que sucessivas, especialmente quando o fato é complexo a exigir investigação diferenciada e contínua. Não configuração de desrespeito ao art. 5º, caput, da L. 9.296/96" (BRASIL. Supremo Tribunal Federal. HC 83515/RS, Pleno, rel. min. Nelson Jobim, j. 16.09.2004, DJ 04.03.2005); "É da jurisprudência desta Corte o entendimento de ser

Entendemos que, para se satisfazer o princípio da proporcionalidade, há que se atender a seu subprincípio denominado exigibilidade temporal, segundo o qual deve haver rigorosa delimitação no tempo da medida coativa[576] e essa delimitação há que estar disciplinada em lei, e não ser entregue à discricionariedade do juiz.

A lei brasileira, que, de fato, até poderia conter redação mais precisa quanto à impossibilidade de sucessivas renovações, há que receber interpretação restritiva em favor do direito individual ao sigilo das comunicações, não se podendo permitir que as interceptações perdurem além do prazo nela estabelecido.

Aliás, segundo interpretação sistemática da Constituição, permitir que renovações da interceptação de comunicações mantenham afastado o direito ao sigilo das comunicações por tempo superior a 60 dias não é razoável por acabar tratando o estado de defesa (art. 136, §1º, I, 'c' e §2º, CF), classificado como o mais grave estado de instabilidade social, com medidas mais brandas do que aquelas dirigidas ao controle da criminalidade comum, ainda que envolvendo crimes violentos, praticados por organizações criminosas ou contra a ordem econômica[577].

---

possível a prorrogação do prazo de autorização para a interceptação telefônica, mesmo que sucessiva, especialmente quando o fato é complexo, a exigir investigação diferenciada e contínua" (BRASIL. Supremo Tribunal Federal. RHC 117467/SP, 1ª T., rel. min. Dias Toffoli, j. 05.11.2013, DJe 22.11.2013); "Persistindo os pressupostos que conduziram à decretação da interceptação telefônica, não há obstáculos para sucessivas prorrogações, desde que devidamente fundamentadas, nem ficam maculadas como ilícitas as provas derivadas da interceptação" (BRASIL. Supremo Tribunal Federal. RHC 85575/SP, rel. min. Joaquim Barbosa, 2ª T., j. 28.03.2006, DJ 16.03.2007); "As autorizações subsequentes de interceptações telefônicas, uma vez evidenciada a necessidade das medidas, não se sujeita a prazo certo, mas ao tempo necessário e razoável para o fim da persecução penal" (BRASIL. Superior Tribunal de Justiça. HC 171910/SP, rel. min. Maria Thereza de Assis, 6ª T., j. 21.11.2013, DJe 09/12/2013); "A Lei n.º 9.296/1996 é explícita quanto ao prazo de quinze dias das escutas telefônicas, bem como a possibilidade da sua renovação. No entanto, segundo a jurisprudência do Superior Tribunal de Justiça, essa aparente limitação do prazo para a realização das interceptações telefônicas não constitui óbice à renovação do pedido de monitoramento telefônico por mais de uma vez" (BRASIL. Superior Tribunal de Justiça. HC 263985/SP, rel. min. Marco Aurélio Bellizze, 5ª T., j. 19.11.2013, DJe 25.11.2013).

[575] Cita-se como exemplo o voto vencido do ministro Marco Aurélio no HC 107521/PR: "Então, tenho como configurado o excesso de prazo. Não conheço a fundamentação do ato, mas esses dois motivos já são suficientes para afastar a preventiva. Quanto às interceptações telefônicas, afirmo, Presidente, que a lei regedora da espécie contém normas imperativas que vinculam o magistrado. Este pode, realmente, deferir a interceptação por quinze dias, prazo prorrogável por idêntico período. Então, não cabe placitar prorrogações sucessivas, tornando a interceptação indeterminada, considerado o fator tempo, quando passa a ser uma verdadeira bisbilhotice, já que, não se levantando dados dentro de trinta dias, geralmente não se faz posteriormente. Portanto, concedo a ordem quanto ao excesso de prazo, quanto à interceptação telefônica relativa a dados angariados após o transcurso dos quinze mais quinze dias, ou seja, após o transcurso dos trinta dias que encerram na lei, como disse, prazo peremptório" (BRASIL. Supremo Tribunal Federal. HC 107521/PR, rel. min. Dias Toffoli, 1ª T., j. 19.02.2013, DJe 22.03.2013).

[576] Sobre os subprincípios do princípio da proporcionalidade, ver item 1.4, *supra*.

[577] PRADO, 2006, p. 39/40. Observe-se, no entanto, que a restrição de direitos passíveis de decretação no estado de defesa não se estende ao sigilo sobre as comunicações telemáticas, mas apenas sobre as telegráficas e telefônicas.

No mesmo sentido da interpretação sistemática suprarreferida, a redação proposta pelo artigo 252 do Projeto de Código de Processo Penal[578] também se mostra excessiva, porquanto fixa o prazo da medida em 60 dias, com possibilidades de tantas prorrogações quantas forem necessárias, até o máximo de 360 dias ou, em caso de crime permanente, até que cesse a permanência.

O aspecto positivo do artigo 252 do Projeto foi a fixação expressa de um limite máximo, ainda que se trate de período muito extenso. Afinal, as evoluções legislativas, muito comumente, precisam percorrer caminhos tortuosos, instituindo retrocessos em alguns aspectos para, noutros, obter a difícil aprovação de avanços, como no exercício de uma árdua e demorada *técnica de construção de garantia*.

Devemos concordar, no entanto, que o prazo estabelecido no artigo 5º da Lei 9.296/96, de quinze dias, prorrogáveis uma vez por igual período, é deveras exíguo, levando a medida da interceptação telemática a se afastar da meta de equilíbrio perseguida na busca de eficiência e garantismo. Daí não se deve extrair, no entanto, a conclusão de que ao intérprete é lícito lançar mão do princípio da proporcionalidade ou de qualquer outro para, aumentando os níveis admitidos por lei para violação de um direito individual, dilatar o prazo de interceptação de comunicações.

Observa-se que, enquanto o prazo legalmente autorizado no Brasil se apresenta exíguo demais, as legislações norte-americana e inglesa promoveram alterações que ampliaram o prazo de forma desmedida, o que não se pode dizer em relação à Espanha, conforme se demonstra abaixo.

Nos Estados Unidos, a lei permite que a interceptação perdure por 30 dias, prorrogáveis por outros 30, sem que haja, porém, limite de quantas prorrogações podem ocorrer. Tal prazo, no entanto, se eleva para um ano em casos de monitoramento de inteligência estrangeira autorizado pelo Presidente da República, sem intervenção judicial, desde que não haja risco de se captar comunicação de alguma "pessoa dos Estados Unidos"[579].

Na Espanha, o *Real Decreto* 424/2005 não conta com qualquer previsão de prazo máximo, ficando este a critério do juiz, que deverá fixá-lo na autorização judicial[580]. Há, no

---

[578] Parecer nº 1.636, de 2010, estabelecendo a redação final do Projeto de Lei do Senado nº 156, de 2009. Disponível em: <http://www.senado.gov.br/atividade/materia/getPDF.asp?t=85509&tp=1>. Acesso em: 24 dez. 2013.
[579] Ver item 3.1.6.
[580] Ver item 3.3.2, *supra*.

entanto, na *Ley de Enjuiciamiento Criminal* e na lei que regula a agência de inteligência espanhola, previsão de prazo de três meses, com possibilidade de sucessivas prorrogações[581].

Já na Inglaterra, o prazo é de três meses, também sem limite para renovações, mas o *Terrorism Act* de 2006 o elevou para seis meses, nos casos que digam respeito à segurança nacional e ao bem-estar econômico do país[582].

A nosso ver, a fixação de prazos excessivamente dilatados, como seis meses ou um ano ou, mesmo a possibilidade de intermináveis prorrogações, mais se parece com um simulacro de cumprimento ao subprincípio da exigibilidade temporal, eis que, em verdade, não se está impondo uma real limitação temporal à medida coativa, mas apenas estabelecendo, de modo meramente formal, números sem qualquer vinculação a uma razoabilidade.

Entendemos, por fim, que, dentre os quatro sistemas analisados, a experiência norte-americana, autorizando a interceptação por 30 dias, se apresenta como a mais equilibrada, exceto pela ausência de limite para as prorrogações e pela possibilidade de interceptação por até um ano quando autorizada pelo Presidente da República. A nosso ver, portanto, 30 dias, prorrogáveis por mais 30 dias, por uma única vez, se apresentaria como um limite capaz de permitir aos sujeitos processuais o exercício adequado de suas faculdades, direitos, garantias e poderes, favorecendo a aproximação da meta de eficiência e garantismo.

4.5 Legitimados a autorizar

O artigo 1º da Lei 9.296/96 estabeleceu que a interceptação de comunicações dependerá de ordem do juiz competente da ação principal, que poderá ser dada, segundo o artigo 3º, a requerimento da autoridade policial e do Ministério Público, além de poder o juiz determiná-la de ofício.

Este tópico abordará três aspectos, quais sejam, a interceptação determinada por CPI, a exigência de que a autorização emane de um juiz e a interceptação determinada de ofício por um juiz.

Os dois primeiros aspectos têm íntima vinculação, na medida em que responder se é ou não imprescindível que a autorização para restringir o sigilo das comunicações de um

[581] Ver item 3.3.2.
[582] Ver item 3.2.3.

indivíduo emane de um juiz, ou se, ao contrário, poderia partir de uma CPI ou de uma autoridade do Executivo, dependerá, em ambos os casos, de verificar se incide ou não na espécie a chamada cláusula de reserva de jurisdição.

No capítulo 3, retratamos outros ordenamentos nos quais a interceptação não depende de intervenção judicial, de modo a que pudéssemos verificar qual das experiências analisadas melhor atende o princípio da proporcionalidade e qual é capaz de chegar mais próximo do pretendido ponto médio entre punição a todo custo e o hipergarantismo, representativo da meta de eficiência e garantismo a se perseguir num processo penal ideal.

Na Inglaterra, a autorização da interceptação compete ao Secretário de Estado, mas, em casos urgentes, poderá ser concedida, também, por um rol de outras autoridades do Executivo[583].

Relevante notar que, naquele país, há, também, previsão expressa de um rol de autoridades que detêm o poder de modificar autorizações de interceptação. Tais autoridades eram, até 2006, as mesmas permitidas por lei a expedir as autorizações originárias, mas o *Terrorism Act* de 2006 veio a ampliar esse rol para casos de risco à segurança nacional, estendendo tal possibilidade ao próprio investigador que porta a autorização[584].

Nos Estados Unidos, embora a autorização deva, tal qual no Brasil, partir de um juiz, a lei permite que qualquer oficial investigador designado pelo procurador geral ou por seus subordinados mais imediatos, em caso de emergência envolvendo perigo imediato de vida, ou de graves danos físicos à pessoa, ou atividades conspiratórias próprias de crime organizado, ou que ameacem a segurança nacional, poderá promover interceptação de comunicações, desde que, dentro de 48 horas, apresente um pedido de aprovação (*approval*) a um juiz[585].

Pode haver, ainda, autorização do Presidente da República para interceptação, sem intervenção judicial, para captar dados de inteligência técnica em comunicações entre poderes estrangeiros ou comunicações advindas de fora do país[586].

Situação semelhante à norte-americana ocorre na Espanha, onde, apesar de caber ao juiz a autorização para interceptar comunicações, há também a previsão de interceptação a ser deferida, em casos urgentes, pelo Ministro do Interior ou pelo Diretor de Segurança do Estado, comunicando-se imediatamente ao juiz, que, dentro de 72 horas, revogará ou manterá o monitoramento[587].

---

[583] Ver item 3.2.3.
[584] Ver item 3.2.3.
[585] Ver item 3.1.6.
[586] Ver item 3.1.6.
[587] Ver item 3.3.2.

No Brasil, tanto o texto constitucional (art. 5º, XII), quanto a lei (art. 3º, Lei 9.296/96) apontam para a exigência de autorização judicial para que se promova uma interceptação de comunicações. Há, por outro lado, previsão constitucional de que as comissões parlamentares de inquérito terão poderes de investigação próprios das autoridades judiciais (art. 58, §3º), o que exige o enfrentamento da divergência de pensamento quanto à possibilidade que elas têm ou não de determinar interceptação de comunicações sem intervenção judicial.

Sabe-se que há situações em que, entre os Poderes Executivo, Legislativo e Judiciário, um exerce funções que tradicionalmente, ou ao menos aparentemente, seriam de outro, verificando-se, portanto, o que se poderia chamar de aparentes invasões mútuas nas áreas de atuação uns dos outros. Exemplos são a sanção, veto e promulgação de leis pelo Presidente da República, além da expedição de decretos (art. 84, IV e V), a aprovação do orçamento dos tribunais pelo Legislativo (art. 99, §2º), as leis de proposta exclusiva do Judiciário (art. 125, §3º), as leis de proposta exclusiva do Executivo (art. 54, §3º), a fixação, pelo Legislativo, dos limites globais para o montante da dívida pública (art. 52, VI), o controle de constitucionalidade das leis pelo Judiciário (art. 102, §2º), o processo e julgamento de determinadas autoridades por crimes de responsabilidade pelo Senado Federal (art. 52, I e II), a fiscalização das contas da administração pública pelo Legislativo (art. 71) e, finalmente, as investigações conduzidas pelas comissões parlamentares de inquérito (art. 58, §3º).

Mas, pela teoria da separação dos poderes, impõe-se um limite a essas invasões mútuas, limite este que procuraremos definir apenas no que se refere à interceptação de comunicações, de modo a verificar se é ou não um meio de obtenção de prova condicionado à cláusula da reserva de jurisdição.

Montesquieu, em seu *Do espírito das leis*, partiu de uma concepção segundo a qual todo aquele dotado de poderes sem limites tende a se corromper, razão pela qual devem ser criados mecanismos que impeçam os abusos[588]. A teoria da separação dos poderes defende que, quando as diversas funções que hão de ser desempenhadas pelo Estado se fazem exercer por órgãos distintos, os cidadãos colhem, como benefício, um mecanismo de controle do arbítrio[589].

Segundo a teoria, a elaboração e alteração das leis gerais e abstratas competiriam ao Legislativo, enquanto que ao Executivo incumbiriam os assuntos de guerra e paz, a defesa da

---

[588] REIS, José Carlos Vasconcellos dos. Controle Externo do Poder Judiciário e separação de poderes. In: QUARESMA, Regina; OLIVEIRA, Maria Lúcia de Paula (Coord.). **Direito Constitucional Brasileiro**: perspectivas e controvérsias contemporâneas. Rio de Janeiro, Forense, 2006, p. 195.

[589] LOWENSTEIN, Karl. **Teoria de la Constitución**. Tradução Alfredo Galego Anabitarte. Barcelona, Ediciones Ariel, 1970, p. 55.

soberania, as relações internacionais e a execução das leis, competindo ao Judiciário, por fim, o julgamento das querelas dos indivíduos e a punição dos crimes[590].

Nessa divisão de tarefas, as legislativas seriam as de criar as leis e as executivas as de aplicá-las, desempenhada tanto pelos tribunais, quanto pela administração[591].

Dos agentes da administração do Estado, integrantes do Executivo, espera-se iniciativa própria, não estando sua atuação condicionada à provocação de quem quer que seja. A eles e às suas funções a parcialidade é inerente, pois o ente estatal que estiver exercendo a função será também parte nas relações a que se referem seus atos, porém uma parte diferente, autoritária, porquanto age com superioridade em relação às demais partes[592].

Já o poder jurisdicional, para ser bem exercido, depende de garantias aos juízes, como a imparcialidade e a independência, razão pela qual cabe a eles juízes a missão de funcionar como os guardiões naturais e primeiros dos direitos fundamentais e das liberdades cidadãs[593], exercendo o papel político social de fiscal da Constituição e garantidor da efetivação dos direitos fundamentais[594].

E da imparcialidade e da independência, emana a isenção, segundo a qual o juiz não poderá atuar com comprometimento com a sociedade ou consigo mesmo[595]. Não poderá estar comprometido com o desejo da maioria, sob o risco de se transfigurar num poder perigoso para minorias e opositores. Tudo isso faz reduzir os riscos de que algum interesse secundário vicie a decisão judicial autorizativa de uma restrição a direito fundamental[596].

Segundo Canotilho, a separação do poder judicial desempenha duas funções: garantir a liberdade, pois não há liberdade quando existir a concentração ou confusão entre quem faz as leis, quem as aplica e quem julga; e garantir a independência da magistratura, pois só magistrados independentes podem assegurar a justiça[597].

Ocorre que, dentro da lógica retratada acima, de que a divisão de tarefas entre poderes conta com aparentes invasões mútuas de áreas de atribuição, ao Legislativo não incumbe tão somente a função de legislar, mas também as de julgar as contas prestadas pelo Presidente da

---

[590] REIS, 2006, p. 198.
[591] CAETANO, Marcello. **Manual de direito administrativo**. Tomo I. 10ª ed. Coimbra: Livraria Almedina, 1982, p. 7/13.
[592] MIRANDA, Jorge. **Teoria do Estado e da Constituição**. Coimbra: Coimbra Editora, 2002, p. 364.
[593] ANTONIO, Ángel Luis Alonso de; ANTONIO, José Antonio Alonso de. **Derecho constitucional español**. 4ª ed. Madrid: Editorial Universitas S.A., 2006, p. 504.
[594] AFONSO, Orlando Viegas Martins. **Poder Judicial**: independência in dependência. Coimbra: Livraria Almedina, 2004, p. 77.
[595] Ibid., p. 50/61. Segundo o mesmo autor, a independência é o que garante a imparcialidade, que, por sua vez, é o que garante a isenção (p. 67).
[596] Ibid., p. 61.
[597] CANOTILHO, 2000, p. 657/658.

República, apreciar os relatórios sobre a execução dos planos de governo e fiscalizar e controlar os atos do Poder Executivo (art. 49, IX e X, CF), controle este que, em nível federal, se faz exercer através do Congresso Nacional, dos Tribunais de Contas e das comissões parlamentares de inquérito.

E esse controle, do Legislativo sobre o Executivo, pode ser classificado como político, fazendo-se nortear pelo critério da oportunidade, o que demonstra o subjetivismo que o cerca[598].

Precisamente quanto às CPIs, elas servem, segundo Paulo Hamilton Siqueira Júnior, para fiscalizar os atos do poder público, investigar irregularidades, abusos e distorções[599]. Tem-se, no entanto, que, concluídos os trabalhos de uma CPI, não poderá ela impor restrições quaisquer aos investigados, já que não é dotada de poder jurisdicional[600].

A nosso ver, não é que os membros do Legislativo e do Executivo, em razão de tudo isso, sejam sempre mais propensos a se vincular a um dos polos de uma contenda ou a um dos interesses em jogo em determinada questão. É muito mais do que isso. A própria natureza de suas posições, de seus cargos, a forma pela qual são escolhidos ou nomeados, o ambiente que cerca a troca de interesses políticos – que, diga-se, poderão ser os mais legítimos, lícitos e verdadeiramente representativos de seu eleitorado – os afastam completamente dos três elementos essenciais àquele que deve desempenhar o papel de zelador das garantias fundamentais: isenção, imparcialidade e independência.

Ademais, aos membros do Executivo e do Legislativo sequer é exigida formação jurídica, que enxergamos como requisito essencial para aquele que for decidir se um indivíduo deve ou não ter seus direitos fundamentais restringidos.

Sob outro aspecto, note-se, ainda, que, se um tribunal for instituído ou um juiz nomeado ou transferido especialmente para julgar um determinado caso, ninguém hesitaria em vislumbrar ferimento à regra do juiz natural (art. 5º, XXXVII e LIII, CF). E a própria forma de instalação de uma CPI, totalmente casuística, voltada sempre para investigar um caso específico, nada mais seria do que, por excelência, uma afronta a essa regra que incide na base da atuação jurisdicional.

Temos, portanto, que, em sendo a interceptação das comunicações telemáticas um meio de obtenção de prova que depende de uma invasão profunda nos direitos fundamentais

---

[598] ANTONIO, 2006, p. 465/474.
[599] SIQUEIRA JÚNIOR, Paulo Hamilton. **Comissão Parlamentar de Inquérito**. Rio de Janeiro, Elsevier, 2007, p. 9.
[600] GONÇALVES, Luiz Carlos dos Santos. **Poderes de investigação das comissões parlamentares de inquérito**. São Paulo: Editora Juarez de Oliveira, 2001, p. 40/41.

do indivíduo, para o que se impõe a atuação de um guardião que ostente os atributos da imparcialidade, independência e isenção, sua implementação está condicionada à cláusula da reserva de jurisdição, não podendo ser determinada por CPI[601] ou, como nas experiências inglesa, norte-americana e espanhola, por autoridades do Poder Executivo.

De mais a mais, agora pontualmente em relação às CPIs, a expressão constitucional "poderes de investigação próprios das autoridades judiciais" há que ser lida tomando-se em consideração que os juízes não detêm, propriamente, *poderes de investigação*. Trata-se, segundo observou, Paulo Ricardo Schier, de um paradoxo constitucional, pois, no mesmo sistema em que se retiram os poderes instrutórios do juiz, acaba-se por conceder "poderes de investigação" aos membros do Poder Legislativo[602], chamando-os de "poderes próprios das autoridades judiciais", que, a bem da verdade, não os detêm.

A mesma lógica levou o Supremo Tribunal Federal a declarar a inconstitucionalidade do artigo 3º da hoje já revogada Lei 9.034/95, que dispunha que o juiz, pessoalmente, realizaria diligência persecutória relativa à investigação de crime organizado, porquanto se entendeu que o juiz não pode desempenhar função investigatória, sob pena de ofensa à sua imparcialidade e ao devido processo legal[603].

Quanto à interceptação das comunicações telemáticas determinada de ofício pelo juiz, o raciocínio é o mesmo. Pende de julgamento pelo Supremo Tribunal Federal a ação direta de inconstitucionalidade nº 3450/DF, proposta pelo Procurador-Geral da República, em que este pugnou pela declaração de inconstitucionalidade do artigo 3º da Lei 9.296/96.

É de se frisar que, se, por um lado, tanto se discute sobre a adequação da iniciativa instrutória do juiz na instrução processual, por outro, essa discussão não ocorre em relação à fase investigatória, na qual eventual iniciativa probatória do juiz tem conotação bem mais grave[604].

---

[601] A jurisprudência do STF, no mesmo sentido, rechaça a possibilidade de interceptação de comunicações determinada por CPI: "A cláusula constitucional da reserva de jurisdição - que incide sobre determinadas matérias, como a busca domiciliar (CF, art. 5º, XI), a interceptação telefônica (CF, art. 5º, XII) e a decretação da prisão de qualquer pessoa, ressalvada a hipótese de flagrância (CF, art. 5º, LXI) - traduz a noção de que, nesses temas específicos, assiste ao Poder Judiciário, não apenas o direito de proferir a última palavra, mas, sobretudo, a prerrogativa de dizer, desde logo, a primeira palavra, excluindo-se, desse modo, por força e autoridade do que dispõe a própria Constituição, a possibilidade do exercício de iguais atribuições, por parte de quaisquer outros órgãos ou autoridades do Estado" (BRASIL. Supremo Tribunal Federal. MS 23452/RJ, rel. min. Celso de Mello, j. 16.09.1999, DJ 12.05.2000).

[602] SCHIER, Paulo Ricardo. As comissões parlamentares de inquérito e a defesa dos direitos individuais. In: **Revista da Acacemia Brasileira de Direito Constitucional**: anais do IV Simpósio Brasileiro de Direito Constitucional, v. 3. Curitiba: ABDC, 2003, p. 277/278.

[603] BRASIL. Supremo Tribunal Federal. ADI 1570-2, rel. min. Maurício Corrêa, Pleno, j. 12.02.2004, DJ 22.10.2004.

[604] "Observe-se, para o processo penal, que é estranha ao tema a questão dos elementos probatórios colhidos durante a investigação prévia e de sua inidoneidade para servir de base à formação do convencimento do juiz.

Para Cervini e Gomes (1997) o artigo 3º é inconstitucional e configurador, tal qual ocorreu com o artigo 3º da Lei 9.034/95, da figura do juiz inquisidor, conflitante com a Constituição e com o modelo acusatório, razão pela qual a iniciativa de buscar a prova compromete o juiz psicologicamente em sua imparcialidade, tornando a prova inadmissível porquanto ilegítima[605].

No mesmo sentido se posiciona Lenio Streck (2001), sustentando que a exigência de imparcialidade, que classificou como uma ficção, porém uma ficção necessariamente útil, tem a função de garantir que o juiz não se comprometerá, de antemão, com nenhum dos contendores, de modo que a determinação da interceptação de ofício macula a instrução processual porquanto choca-se com o moderno processo penal acusatório[606].

Atento a isso, o Projeto de Código de Processo Penal cuidou de suprimir a possibilidade de interceptação determinada de ofício pelo juiz[607], além de ter transferido a competência para autorizá-la ao chamado juiz das garantias[608], concebido para controlar a legalidade da investigação criminal, a ele cabendo apreciar os pedidos de diligências dependentes de ordem judicial e, com isso, evitar que a imparcialidade do juiz que irá julgar a futura ação penal sofra arranhões decorrentes de seu envolvimento psicológico com a investigação.

Observa Rubens Casara que o juiz das garantias deve resistir à tentação de coadjuvar a persecução penal ou mesmo as políticas de segurança pública, não podendo degradar-se em

---

Não se confunda a iniciativa instrutória do juiz *no processo* com a atribuição de poderes de busca da prova *na fase de investigação*. Durante esta, o juiz só pode ter os poderes de determinar medidas cautelares, sob pena de voltar-se à figura do juiz-inquisidor do processo antigo. **r)** Não há razão para se retirar do juiz a iniciativa instrutória, mesmo no processo civil que verse sobre direitos disponíveis. A disponibilidade do direito material não influi sobre o processo que, como instrumento da função estatal, tem invariavelmente natureza pública e função social. O papel ativo do juiz na produção da prova não afeta a liberdade das partes, que podem renunciar, transigir, desistir. Mas a solução processual está nas mãos do juiz, que não pode por isso ser obrigado a satisfazer-se com a atividade instrutória das partes, mesmo no processo civil dispositivo." (GRINOVER, 1999, p. 78).

[605] GOMES; CERVINI, 1997, p. 199, 201 e 205.

[606] STRECK, 2001, p. 81/82.

[607] "Art. 249. O pedido de interceptação de comunicações telefônicas será formulado por escrito ao juiz competente, mediante requerimento do Ministério Público ou da defesa, ou por meio de representação do delegado de polícia, ouvido, neste caso, o Ministério Público, e deverá conter ..." (Parecer nº 1.636, de 2010, estabelecendo a redação final do Projeto de Lei do Senado nº 156, de 2009. Disponível em: <http://www.senado.gov.br/atividade/materia/getPDF.asp?t=85509&tp=1>. Acesso em: 30 dez. 2013).

[608] "Capítulo II. Do juiz das garantias. Art. 14. O juiz das garantias é responsável pelo controle da legalidade da investigação criminal e pela salvaguarda dos direitos individuais cuja franquia tenha sido reservada à autorização prévia do Poder Judiciário, competindo-lhe especialmente: ... XI – decidir sobre os pedidos de: ... a) interceptação telefônica, do fluxo de comunicações em sistemas de informática e telemática ou de outras formas de comunicação" (Parecer .º 1.636, de 2010, estabelecendo a redação final do Projeto de Lei do Senado nº 156, de 2009. Disponível em: <http://www.senado.gov.br/atividade/materia/getPDF.asp?t=85509&tp=1>. Acesso em: 30 dez. 2013).

simples validador de atuações alheias que faça da intervenção judicial puro trâmite colateral da atuação policial, como ocorre com demasiada frequência[609].

Diz o autor, ainda, que, diante da relevância dos interesses em jogo, normalmente direitos fundamentais, a atuação do juiz das garantias também deve estar cercada de garantias tanto orgânicas (voltadas a assegurar a independência dos magistrados, relativas à formação do juiz e à sua colocação institucional em relação aos poderes do Estado e aos outros sujeitos do processo, dentre as quais a inamovibilidade) quanto processuais (direcionadas à limitação do poder das agências estatais), pois a própria existência de um juiz das garantias é, em si, uma garantia, umbilicalmente ligada às garantias do juiz natural e da imparcialidade, mas que só se concretiza se o juiz que exercer a função tiver condições de fazê-lo, sem que fique sujeito a transferências arbitrárias ou designações fundadas em interesses privados[610].

Entendemos, assim, que a decisão de restringir o direito fundamental ao sigilo das comunicações e, junto com ele, à intimidade e à privacidade não pode caber a uma CPI ou, menos ainda, a um membro do Poder Executivo, sob pena de faltar a necessária imparcialidade, integrante do núcleo essencial de garantias[611]. Podemos afirmar, por fim, que os sistemas espanhol, norte-americano e principalmente o inglês destinam, no que se refere às autoridades que podem deferir interceptação de comunicações telemáticas, tratamento que se encontra mais distanciado da meta de eficiência e garantismo do que o do Brasil.

Concluímos, também, que o juiz não pode determinar interceptação de comunicações de ofício, tendo em vista que lhe subtrairia a imparcialidade, ofendendo o núcleo essencial de garantias.

4.6 Legitimados a requerer e a promover interceptação

Nos termos da Lei 9.296/96, a interceptação pode ser implementada a requerimento do Ministério Público, na investigação criminal e na instrução processual penal (art. 3º, II), bem como da autoridade policial, na investigação criminal (art. 3º, I).

---

[609] CASARA, Rubens R. R. Juiz das garantias: entre uma missão de liberdade e o contexto de repressão. In: COUTINHO, Jacinto Nelson de Miranda; CARVALHO, Luis Gostavo Grandinetti Castanho de (Org.). **O novo processo penal à luz da Constituição**: análise crítica do Projeto de Lei nº 156/2009, do Senado Federal. Rio de Janeiro: Lumen Juris, 2010, p. 170.

[610] CASARA, 2010, p. 171 e 176.

[611] Sobre o conceito de núcleo essencial de garantias, ver item 1.4.

O Projeto de Código de Processo Penal acresce a defesa entre os legitimados a requerer interceptação ao juiz (art. 249)[612], o que já era um antigo anseio da doutrina.

Para Luiz Flavio Gomes e Raúl Cervini (1997), a defesa já poderia, mesmo na vigência da lei atual, com fulcro no princípio da paridade de tratamento, pedir interceptação para defender um suspeito ou acusado, pois a Constituição restringiu a medida para fins criminais mas não distinguiu se em favor da acusação ou da defesa[613].

Lenio Streck (2001) entende que a lei deveria ter assegurado também à defesa o direito de requerer a interceptação das comunicações de terceiros que tenham relação com o processo, como a vítima e as testemunhas de acusação, caso haja indícios de que tenham faltado com a verdade ou omitido dados importantes para o processo. Sustenta que a não contemplação da defesa dentre os legitimados a requerer a medida torna o artigo 3º violador dos princípios da ampla defesa e do contraditório, pelo que, numa interpretação conforme a Constituição, deve-se, desde já, admitir que também a defesa possa requerê-la[614].

Nas propostas e críticas do Instituto Brasileiro de Direito Processual (IBDP) ao Projeto de CPP, sugeriu-se que, dentre os legitimados, figurassem também o querelante e o suspeito, o primeiro para sustentar sua acusação e o último para exercer seu direito de defesa[615].

Quanto às vítimas em geral, Luiz Flavio Gomes e Raúl Cervini (1997) entendem que a elas a lei não conferiu a possibilidade de requererem diretamente interceptação, nada impedindo, no entanto, que formulem sugestão à autoridade policial ou ao Ministério Público para que se requeira a medida. Já nas ações penais privadas, entendem os autores que poderá o querelante requerer diretamente a medida de interceptação[616].

Responder se à defesa deve ou não ser assegurado o direito a pleitear a interceptação das comunicações de vítimas, testemunhas ou terceiros passa pela verificação quanto ao cabimento da investigação defensiva, bem como quanto à incidência de contraditório e ampla defesa na fase investigatória.

Ao réu e autor devem-se assegurar os mesmos direitos, os mesmos ônus e os mesmos deveres, de modo a garantir-lhes uma paridade de armas capaz de igualá-los no processo. De tal assertiva, todavia, não se extrai que, em determinadas situações, não possa haver

---

[612] Parecer nº 1.636, de 2010, estabelecendo a redação final do Projeto de Lei do Senado nº 156, de 2009. Disponível em: <http://www.senado.gov.br/atividade/materia/getPDF.asp?t=85509&tp=1>. Acesso em: 31 dez. 2013.
[613] GOMES; CERVINI, 1997, p. 209.
[614] STRECK, 2001, p. 79/81.
[615] INSTITUTO BRASILERO DE DIREITO PROCESSUAL (IBDP). Propostas de emendas ao Projeto de Lei de Código de Processo Penal. Substitutivo CCJ do Senado. Disponível em: <http://www.direitoprocessual.org.br/download.php?f=9546b22fe462eb3d2116f6ff5b62a312>. Acesso em: 31 dez. 2013.
[616] GOMES; CERVINI, 1997, p. 209.

tratamento especial, mas tal tratamento especial servirá justamente para compensar eventuais desigualdades e, suprindo o desnível da parte inferiorizada, assegurar a paridade de armas[617].

Um dos exemplos deste desnível é o fato de que a acusação conta com todo o aparelho estatal montado para ampará-la, enquanto o acusado conta somente com suas próprias forças e com o auxílio de seu advogado, o que explicaria a concepção de princípios como o *in dubio pro reo* e o *favor rei*[618].

Antigo é o posicionamento doutrinário no sentido de que o inquérito policial é inquisitório[619] e de que nele não é permitido ao investigado exercer o contraditório, de modo a ficar a critério da autoridade policial as oitivas e diligências por ele requeridas, sob pena de que o suspeito venha a tumultuar o trabalho da polícia judiciária[620].

Joaquim Canuto Mendes de Almeida (1973), classificando o suspeito como sujeito de direitos (e não mero objeto de investigação), afirma que seria contrário a qualquer senso de justiça afastar da investigação justamente a pessoa do investigado, como se ele nada tivesse a ver com sua própria liberdade, até porque será da investigação que se extrairá a base para a deflagração da ação penal[621]. Para este autor, no entanto, a necessidade de que se assegure ao suspeito a possibilidade de se defender na investigação não importa em garantir-lhe o exercício de contraditório, já que nesta fase não caberia intervenção ampla das partes[622].

Para Antonio Scarance Fernandes (2010), há, sem dúvida, que se admitir atuação da defesa na investigação, ainda que nela não haja contraditório ou a obrigatoriedade de se intimar o suspeito dos atos a serem realizados, não se tratando, pois, de defesa ampla, mas de defesa limitada ao resguardo dos interesses mais relevantes do suspeito, como o requerimento de diligências, o pedido de liberdade provisória, de relaxamento de flagrante e a impetração de *habeas corpus*[623].

Já para Rogério Lauria Tucci, a contraditoriedade, calcada na tradicionalizada parêmia *aldiatur et altera pars*, se impõe em toda a instrução criminal, seja ela pré-processual, seja

---

[617] FERNANDES, 2010, p. 48.
[618] Ibid., p. 49.
[619] GRECO FILHO, Vicente. **Manual de processo penal**. 7ª ed., São Paulo: Saraiva, 2009, p. 77; TOURINHO FILHO, Fernando da Costa. **Manual de processo penal**. 8ª ed. São Paulo: Saraiva, 2006, p. 68; MARQUES, José Frederico. **Tratado de direito processual penal**. v. I. São Paulo: Saraiva, 1980, p. 190; FERNANDES, 2010, 64.
[620] MARQUES, José Frederico, **Elementos de direito processual penal**. v. I. Campinas: Bookseller, 1997, p. 151.
[621] ALMEIDA, Joaquim Canuto Mendes de. **Princípios fundamentais do processo penal**. São Paulo: Revista dos Tribunais, 1973, p. 217.
[622] Ibid., p. 116/117.
[623] FERNANDES, 2010, p. 63: O autor destaca a Lei 11.449/2007 como importante norma que veio a assegurar a atuação da defesa na fase pré-processual, por força da qual deverá ser remetida cópia do auto de prisão em flagrante à Defensoria Pública.

realizada em juízo, a fim de que o órgão jurisdicional competente, devidamente formado o seu convencimento, possa pronunciar-se o mais corretamente possível e com justiça[624].

Assim, mesmo a corrente que não admite a incidência de contraditório na fase investigatória concorda que o suspeito possui direito de defesa, já que se trata de um sujeito de direitos colocado na delicada posição de criminalmente investigado[625], com todos os riscos dela advindos. Ademais, como bem observou Antonio Magalhães Gomes Filho, determinadas provas colhidas na fase administrativa, como as periciais, por sua natureza urgente, já são realizadas definitivamente no inquérito, sujeitando-se apenas a um controle contraditório *a posteriori*, nem sempre efetivo e suficiente para a garantia da defesa[626].

Aliás, um exemplo clássico de prova colhida definitivamente na fase pré-processual é aquela decorrente de interceptação das comunicações, tendo em vista que, por óbvio, registra um momento único, passível de captação um única vez[627].

A nosso ver, não incide o contraditório na fase investigatória, não existindo obrigatoriedade de que se intime o investigado a se manifestar ou de que se lhe dê ciência dos atos já praticados ou dos futuros, tendo em vista não se coadunar com o momento investigatório prévio, que não comporta a exigência de bilateralidade de audiência por razões de celeridade.

Há, no entanto, que se assegurar à defesa a possibilidade de, buscando fazer-se efetiva, investigar e requerer os atos investigatórios necessários à sustentação das alegações do suspeito, o que fará nascer para autoridade policial, em contrapartida, um dever de apreciar, motivadamente, o requerimento defensivo, sob pena de se pender a balança para o lado da acusação (da futura acusação), tornando-se desiguais as forças das partes (na futura instrução processual) e se quebrando o núcleo essencial de garantias em razão de violação à ampla defesa.

Eventual desconsideração de tal requerimento por parte da autoridade policial, ou seu desacolhimento imotivado, deve ser passível de impugnação através de *habeas corpus* ou, em tempos de restrição exacerbada de seu cabimento[628], mandado de segurança.

---

[624] TUCCI, 2009, p. 160/161.

[625] PITOMBO, Sergio Marcos de Moraes. Inquérito policial: exercício do direito de defesa. **Boletim do Instituto Brasileiro de Ciências Criminais**, São Paulo, nº 83. edição especial. Out/1999, p. 14.

[626] GOMES FILHO, 1997, p. 144/145.

[627] Com tal registro, no entanto, não estamos sustentando que o suspeito deve poder se defender da interceptação durante sua realização, mas apenas exemplificando prova irrepetível produzida na fase pré-processual, a corroborar a necessidade de que o investigado possa praticar atos de defesa em tal fase.

[628] O mais recente *leading case* a restringir a amplitude do cabimento do *habeas corpus* emanou da 1ª Turma do Supremo Tribunal Federal, no HC 109.956/PR (rel. min. Marco Aurélio, 1ª T., j. 14.08.2012, DJ 11.09.2012).

Mas, dentre os demais legitimados a requerer e implementar a medida, observa-se uma peculiaridade no que diz respeito à defesa, e também à vítima, porquanto se trate de particulares. Isto porque não há regulamentação legal suficiente para disciplinar a realização de uma interceptação defensiva ou interceptação pelo querelante.

É de se recordar que, na Inglaterra, uma das principais preocupações do Parlamento em relação à promessa que o então recém-eleito governo Thatcher fizera de privatizar os serviços de telecomunicações estatais, e que levou o Legislativo a, açodadamente, aprovar o *Telecommunications Act* de 1984, foi a de que, uma vez privatizado o setor, as medidas de interceptação telefônica, atividade eminentemente estatal, dependeriam da manipulação ou da colaboração de particulares, inexistindo a previsão de mecanismos de controle e disciplina legal para tanto[629].

De fato, parece-nos legítima a preocupação com a possibilidade de que particulares violem o sigilo de comunicações, ainda que por força de determinação legal, sem a existência de um regulamento detalhado e restritivo. Por tal razão, não se imagina que o defensor, no Brasil ou onde quer que seja, possa, ele próprio, implementar interceptação de comunicações que lhe tenha sido deferida. A interceptação, portanto, deveria ser implementada pela polícia com a previsão de mecanismos que permitam o acompanhamento pela defesa, interessada em sua realização.

Em termos de previsão legal da investigação defensiva no Brasil, Gustavo Badaró (2012) observa que a norma do artigo 14 do CPP[630] é claramente insuficiente, até porque o advogado não dispõe de meios de intimar alguém para depor em seu escritório, além do que qualquer expediente no sentido de travar contato prévio com testemunhas pode ser visto como ferimento a normas deontológicas da profissão advocatícia ou, quiçá, prática de crime[631].

Já nos Estados Unidos, o direito a uma investigação defensiva emana da Sexta Emenda[632], no trecho que assegura o direito a ser assistido por um defensor (*assistance of counsel for his defense*), o que, do ponto de vista da atividade advocatícia e de suas

---

[629] Ver item 3.2.2.

[630] Art. 14. O ofendido, ou seu representante legal, e o indiciado poderão requerer qualquer diligência, que será realizada, ou não, a juízo da autoridade.

[631] BADARÓ, 2012, p. 95/96.

[632] Sixth Amendment. In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the state and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the assistance of counsel for his defense. Disponível em: <http://www.law.cornell.edu/constitution/sixth_amendment>. Acesso em: 03 jan. 2014.

obrigações deontológicas, inclui um dever de investigar (*duty to investigate*), de modo a que este realize uma defesa efetiva[633].

Naquele país, inclusive, há uma cultura das partes de preferirem produzir as provas pré-processuais de forma particular para, somente depois, inseri-las no processo na forma documental, em razão da onerosidade da Justiça criminal, sendo comum que escritórios de advocacia e até as próprias promotorias tenham notários para auxiliá-los na tomada de depoimentos[634].

Na Itália, de forma mais satisfatória, os artigos 391-bis a 391-decies do CPP preveem, como atos cabíveis na investigação defensiva, a conversa informal com testemunhas, o pedido de declaração escrita a testemunhas, a obtenção de declarações de testemunha registradas documentalmente, a requisição de documentos à administração pública, o acesso a locais públicos ou abertos ao público para verificação do estado do lugar ou de coisas, o acesso a lugares privados ou não abertos ao público desde que haja concordância de quem tenha disponibilidade sobre o lugar ou autorização judicial[635].

Assim, é necessária, no Brasil, a aprovação de dispositivo legal regulamentando a participação defensiva, pois, se for ela a requerer a medida e não podendo ser ela própria a implementá-la, há que haver uma forma de ela acompanhar, ainda que a distância, a captação gradual das comunicações de seu interesse.

Quanto à vítima ou ao querelante, entendemos que a mesma possibilidade, de requerer interceptação, deve ser a ele assegurada, em razão do que poderíamos chamar de uma forte tendência legislativa no sentido de aumentar o prestígio e as prerrogativas processuais das vítimas.

O primeiro sinal desta tendência legislativa está no fato de não ser taxativo o rol de personagens que podem funcionar como assistentes de acusação estabelecido no artigo 268 do CPP[636], pois outros diplomas posteriores vieram a admitir a atuação do assistente de acusação noutras hipóteses, a saber, nos crimes contra o consumidor[637], contra o sistema financeiro nacional[638] e contra a propriedade imaterial[639].

---

[633] BADARÓ, 2012, p. 96.

[634] RAMOS, João Gualberto Garcez. **Curso de processo penal norte-americano**. São Paulo: Revista dos Tribunais, 2006, p. 190/191.

[635] BADARÓ, 2012, p. 96, nota nº 78.

[636] CPP. Art. 268. Em todos os termos da ação pública, poderá intervir, como assistente do Ministério Público, o ofendido ou seu representante legal, ou, na falta, qualquer das pessoas mencionadas no Art. 31.

[637] Lei 8.078/90. Art. 80. No processo penal atinente aos crimes previstos neste código, bem como a outros crimes e contravenções que envolvam relações de consumo, poderão intervir, como assistentes do Ministério Público, os legitimados indicados no art. 82, inciso III e IV, aos quais também é facultado propor ação penal subsidiária, se a denúncia não for oferecida no prazo legal. ... Art. 82. Para os fins do art. 81, parágrafo único, são legitimados concorrentemente: (Redação dada pela Lei nº 9.008, de 21.3.1995) ... III - as entidades e órgãos

A Lei 9.099/95 foi, talvez, o maior marco na trajetória legislativa brasileira rumo ao aumento da participação da vítima no processo penal, ao estabelecer, como uma das metas dos Juizados Especiais Criminais, a reparação dos danos sofridos por ela[640] e ao instituir a composição civil dos danos, que, nos crimes de ação penal privada ou condicionada à representação, fez entregar nas mãos da vítima a prerrogativa de fazer cessar a persecução penal em troca de um benefício ou uma vantagem de sua escolha[641].

Observe-se, ainda, que, mesmo quando diante de crime de ação pública incondicionada, a praxe dos Juizados Especiais Criminais já se consolidou no sentido de acatar o desejo da vítima de dar fim à ação penal, conforme se extrai do Enunciado nº 99, concebido no XXIII Encontro de Juízes de Juizados Especiais[642].

Dita tendência de valorização ao papel da vítima se evidencia, ainda, na reparação do dano como causa extintiva da punibilidade de crimes fiscais e previdenciários (art. 69, Lei 11.941/09); na multa reparatória (art. 297, Lei 9.503/97); na pena de prestação pecuniária e nos incentivos para a reparação do dano (art. 12, Lei 9.605/98 e art. 45, §1º do Código Penal, instituído pela Lei 9.714/98); na lei de proteção a testemunhas e vítimas ameaçadas (Lei 9.807/99); e no capítulo inteiro inserido no CPP (Capítulo V do Título VII do CPP, introduzido pela Lei 11.690/08), que veio a assegurar às vítimas diversos direitos, a exemplo da ciência sobre o ingresso e saída do réu da prisão, datas de audiências, sentença e acórdãos que a modifiquem, espaço a elas reservado no ambiente forense, atendimento psicossocial,

---

da Administração Pública, direta ou indireta, ainda que sem personalidade jurídica, especificamente destinados à defesa dos interesses e direitos protegidos por este código; IV - as associações legalmente constituídas há pelo menos um ano e que incluam entre seus fins institucionais a defesa dos interesses e direitos protegidos por este código, dispensada a autorização assemblear.

[638] Lei 7492/86. Art. 26. A ação penal, nos crimes previstos nesta lei, será promovida pelo Ministério Público Federal, perante a Justiça Federal. Parágrafo único. Sem prejuízo do disposto no art. 268 do Código de Processo Penal, aprovado pelo Decreto-lei nº 3.689, de 3 de outubro de 1941, será admitida a assistência da Comissão de Valores Mobiliários - CVM, quando o crime tiver sido praticado no âmbito de atividade sujeita à disciplina e à fiscalização dessa Autarquia, e do Banco Central do Brasil quando, fora daquela hipótese, houver sido cometido na órbita de atividade sujeita à sua disciplina e fiscalização.

[639] CPP. Art. 530-H. As associações de titulares de direitos de autor e os que lhes são conexos poderão, em seu próprio nome, funcionar como assistente da acusação nos crimes previstos no art. 184 do Código Penal, quando praticado em detrimento de qualquer de seus associados. (Incluído pela Lei nº 10.695, de 1º.7.2003).

[640] Lei 9.099/95. Art. 62. O processo perante o Juizado Especial orientar-se-á pelos critérios da oralidade, informalidade, economia processual e celeridade, objetivando, sempre que possível, a reparação dos danos sofridos pela vítima e a aplicação de pena não privativa de liberdade.

[641] Lei 9.099/95. Art. 74. A composição dos danos civis será reduzida a escrito e, homologada pelo Juiz mediante sentença irrecorrível, terá eficácia de título a ser executado no juízo civil competente. Parágrafo único. Tratando-se de ação penal de iniciativa privada ou de ação penal pública condicionada à representação, o acordo homologado acarreta a renúncia ao direito de queixa ou representação.

[642] Enunciado nº 99 do XXIII Encontro de Juízes de Juizados Especiais (Boa Vista, RR): "Nas infrações penais em que haja vítima determinada, em caso de desinteresse desta ou de composição civil, deixa de existir justa causa para ação penal" (BRASIL. Tribunal de Justiça do Estado do Rio de Janeiro. Juizados Especiais: enunciados e recomendações do PJERJ. Ato TJ nº SN12, de 23.06.2010. Disponível em: <http://portaltj.tjrj.jus.br/documents/10136/30422/juizados-especiais.pdf>. Acesso em: 11.12.2013).

jurídico e de saúde, a expensas do ofensor ou do Estado, bem como a preservação de sua intimidade, vida privada, honra e imagem, podendo ensejar, inclusive, decreto de segredo de justiça no feito.

Também a Lei 11.719/08 acresceu o inciso VII ao artigo 387 do CPP[643], estabelecendo que a sentença penal condenatória fixará, desde logo, valor mínimo para reparação dos prejuízos sofridos pelo ofendido, a serem executados na forma do artigo 63[644].

Estas medidas são voltadas para evitar o que os criminólogos chamam de "vitimização secundária", decorrente do pouco caso ou inoperância por parte do Estado para com as vítimas[645].

Concordamos, portanto, com a legitimidade da defesa e da vítima para requerer (mas não para implementar) interceptação de comunicações, devendo haver um procedimento pelo qual o interessado na prova, em sendo particular, possa acompanhar sua colheita, a ser realizada pela polícia.

Ainda tratando dos legitimados a requerer e a implementar interceptação de comunicações, há um aspecto que tem passado desapercebido pelos doutrinadores que tratam do tema.

Trata-se da possibilidade ou impossibilidade de que a medida de interceptação seja requerida e realizada pela Agência Brasileira de Inteligência (ABIN), que não figura dentre os legitimados do artigo 3º da Lei 9.296/96, mas que tem, dentre suas missões institucionais, a "obtenção, análise e disseminação de conhecimentos dentro e fora do território nacional sobre fatos e situações de imediata ou potencial influência sobre o processo decisório e a ação governamental e sobre a salvaguarda e a segurança da sociedade e do Estado"[646].

Há, diante disso, uma espécie de anseio institucional para que a ABIN possa, tal qual outras agências de inteligência, lançar mão da interceptação das comunicações para melhor

---

[643] CPP. Art. 387. O juiz, ao proferir sentença condenatória: (Vide Lei nº 11.719, de 2008) ... IV - fixará valor mínimo para reparação dos danos causados pela infração, considerando os prejuízos sofridos pelo ofendido; (Redação dada pela Lei nº 11.719, de 2008).

[644] CPP. Art. 63. Transitada em julgado a sentença condenatória, poderão promover-lhe a execução, no juízo cível, para o efeito da reparação do dano, o ofendido, seu representante legal ou seus herdeiros. Parágrafo único. Transitada em julgado a sentença condenatória, a execução poderá ser efetuada pelo valor fixado nos termos do inciso IV do caput do art. 387 deste Código sem prejuízo da liquidação para a apuração do dano efetivamente sofrido. (Incluído pela Lei nº 11.719, de 2008).

[645] BIANCHINI, Alice. **Falta de delegacias especializadas**: outra forma de violência contra a mulher. Disponível em: <http://ww3.lfg.com.br/public_html/article.php?story=201103151453246&mode=print>. Acesso em: 03 jan. 2014.

[646] Lei 9.883/99 - Institui o Sistema Brasileiro de Inteligência, cria a Agência Brasileira de Inteligência - ABIN, e dá outras providências. Art. 1º. ... § 2º Para os efeitos de aplicação desta Lei, entende-se como inteligência a atividade que objetiva a obtenção, análise e disseminação de conhecimentos dentro e fora do território nacional sobre fatos e situações de imediata ou potencial influência sobre o processo decisório e a ação governamental e sobre a salvaguarda e a segurança da sociedade e do Estado.

cumprir seu múnus legal, adotando-a, por exemplo, como medida preventiva contra suspeitos de planejar atos terroristas[647].

Fabio Condeixa (2014) observa que, muito embora, os estrangeiros não residentes façam jus a diversos direitos, a exemplo da ampla defesa e da liberdade, assegurados pela Convenção Americana de Direitos Humanos, não fariam eles jus ao direito ao sigilo das comunicações, porquanto o *caput* do artigo 5º da Constituição restringiria os direitos previstos em seus incisos "aos brasileiros e aos estrangeiros residentes no País". Com este raciocínio, o autor advoga a possibilidade que a ABIN promova interceptações de estrangeiros não residentes sem ordem judicial, uma vez que estes não seriam destinatários do direito à inviolabilidade do sigilo das comunicações previsto no inciso XII[648].

É verdade que Estados Unidos e Inglaterra preveem modalidades de interceptação à qual estão sujeitos somente alvos estrangeiros ou, mais precisamente, no primeiro caso, quem que não ostente a condição de "pessoa dos Estados Unidos"[649] ou, no segundo, quem esteja "fora das Ilhas Britânicas"[650].

Na Espanha, conforme retratado no item 3.3.2, o *Centro Nacional de Inteligencia* pode pedir autorização ao *Tribunal Supremo* para promover interceptações, que, no entanto, não terão natureza criminal, já que as investigações conduzidas pela dita agência de inteligência não têm por objeto a investigação de crimes, mas sim os temas próprios de agências governamentais de inteligência, a exemplo, tal qual elencado no artigo 4º da *Ley* 11/2002, da obtenção e avaliação de informações para proteger os interesses políticos, nacionais, econômicos, industriais, comerciais e estratégicos da Espanha.

Quanto à brasileira ABIN, não endossamos o raciocínio excludente de estrangeiros não residentes no País do grupo de beneficiários dos direitos e garantias individuais estabelecidos no artigo 5º da Constituição[651]. Tão pouco subscrevemos a possibilidade de que a Agência intercepte sem ordem judicial.

No entanto, é inegável que a legislação e a própria Constituição deveriam ter permitido à ABIN lançar mão desse instrumento, ainda que para fins não penais, mas desde

---

[647] CONDEIXA, Fábio de Macedo Soares Pires. Interceptações das comunicações de estrangeiros não residentes: Wiretapping of non-resident aliens. In: **Programa de Estudos em Criminologia e Ciências Penitenciárias – PROCRIM**, São Paulo, ano 3, nº 04, dezembro/2013/ferereiro/2014, p. 11.
[648] Ibid., p. 8.
[649] Ver item 3.1.6.
[650] Ver item 3.2.3.
[651] Conforme observado no item 3.2.3, o STF já decidiu no sentido de que, no que se refere ao rol de direitos fundamentais da CF, não há distinção entre o estrangeiro não residente e o brasileiro.

que servindo a relevantes interesses nacionais[652]. Afinal, se as experiências inglesa e norte-americana mostraram que seus ordenamentos baixam a barricada protetora de estrangeiros, o que inclui os brasileiros, e, para além disso, se o escândalo Snowden mostrou que governos estrangeiros têm lançando mão de espionagem contra outros governos, inclusive contra o brasileiro, visando, muitas vezes, informações puramente comerciais e estratégicas[653], não é razoável colocar o serviço de inteligência brasileiro e o próprio Brasil em franca desvantagem ou tendo que atuar na ilegalidade. Embora se colha desta prática ofensa até mesmo ao princípio da reciprocidade, não advogamos a sonegação dos direitos fundamentais aos não residentes no Brasil, mas entendemos que os termos da lei e da Constituição teriam andado melhor se assegurassem a possibilidade de interceptação pela ABIN (o que não ocorreu).

4.7 A inutilização das comunicações que não interessarem à prova

O artigo 9º da Lei 9.296/96 dispõe que a gravação que não interessar à prova será inutilizada por decisão judicial, durante o inquérito, a instrução processual ou após esta, em virtude de requerimento do Ministério Público ou da parte interessada. Seu parágrafo único prevê que o incidente de inutilização será assistido pelo Ministério Público, sendo facultada a presença do acusado ou de seu representante legal.

Luiz Flavio Gomes e Raúl Cervini (1997) sustentam que, uma vez constatada a inutilidade, o material deve ser inutilizado imediatamente, pois o que é inútil para o processo penal pode chegar a destruir uma vida se revelado, tudo de modo a tutelar real e efetivamente o direito à intimidade e ao sigilo das comunicações. Entendem que também as referências às comunicações tidas por inservíveis devem ser inutilizadas, tais como os autos circunstanciados e as transcrições, bem como que a seleção final do que interessa ou não à prova caberá ao juiz, no exercício do controle judicial da interceptação. No incidente de inutilização, entendem obrigatória a presença do órgão de acusação, mas facultativa a presença da defesa[654].

Vicente Greco Filho (1996) sustenta que o incidente de inutilização deve ser assistido pelo Ministério Público, porquanto fiscal da lei e do interesse público, sendo facultada a

[652] Quanto à possibilidade de que se promova no Brasil interceptação com fins preventivos, ou seja, para prevenir um crime, ver item 4.12.
[653] Ver item 2.2.1.
[654] GOMES; CERVINI, 1997, p. 233/236.

presença do acusado ou seu defensor, somente se a inutilização se realizar depois de instaurada a ação penal, pois, caso esta se dê na fase preliminar, não haverá que se falar em presença do acusado[655].

Já Ada Pellegrini, Gomes Filho e Scarance Fernandes (2009) observam ser evidente a inconstitucionalidade da expressão "facultada", porquanto é imprescindível a presença do acusado, bem como de seu defensor no momento da realização do incidente de inutilização, de modo a assegurar a autodefesa e a defesa técnica[656].

Há que se notar que a destruição de uma determinada parte do que se amealhou por meio da interceptação constitui, tão simplesmente, uma forma de seleção do que será aproveitado como prova e do que será excluído do processo, o que permite inferir a relevância do ato, a importância, enfim, do momento processual.

A expressão *cadeia de custódia* costuma ser muito utilizada em processo penal quando se está tratando de vestígios médico-legais, de amostras para análises toxicológicas forenses, havendo uma justa preocupação com o transporte, armazenamento e registro de cada profissional que manipulou o material. Mas pouco se fala em cadeia de custódia quando não se está tratando de criminalística.

Em publicação sobre o processo penal costa-riquenho, Federico Campos (2002) observou que, caso se descumpra, dolosa ou culposamente, os procedimentos técnicos específicos para o manejo da prova, estar-se-ia diante de uma atividade processual defeituosa, cuja consequência processual seria a conversão dos indícios probatórios em prova ilícita ou espúria, ante a existência de defeito absoluto[657].

Todos os procedimentos relacionados à evidência, desde a coleta, o manuseio e análise, sem os devidos cuidados e sem a observação de condições mínimas de segurança, podem acarretar a falta de integridade da prova, provocando danos irrecuperáveis no material coletado, comprometendo a idoneidade do processo e prejudicando a sua rastreabilidade[658].

---

[655] GRECO FILHO, 1996, p. 34.
[656] GRINOVER; GOMES FILHO; FERNANDES, 2009, p. 179.
[657] "Ante el supuesto de que en la investigación judicial los sujetos intervinientes en el manejo de la evidencia no respeten – ya sea en forma dolosa o imprudente – los procedimientos técnicos específicos, estaremos razonablemente en presencia de una actividad procesal defectuosa (arts. 175 y sts. Código Procesal Penal, en adelante CPP), cuya consecuencia procesal inmediata sería la conversión de esos indicios probatorios en prueba ilícita o espuria por la existencia de un defecto absoluto" (CAMPOS, Federico. **La relevancia de la custodia de la evidencia en la investigación judicial**. Medicina Legal de Costa Rica, vol. 19, nº 1, Heredia mar. 2002. Disponível em: <http://www.scielo.sa.cr/scielo.php?script=sci_arttext&pid=S1409-00152002000100008&lng=es&nrm=iso>. Acesso em: 04 jan. 2014).
[658] GABRIEL, Maria Madalena; LOPES, M; BARETA, G. M. S. **Cadeia de Custódia:** uma abordagem preliminar. 2006. Disponível em: <http://ojs.c3sl.ufpr.br/ojs2/index.php/academica/article/view/9022/6315>. Acesso em: 04 jan. 2014.

Mas também a prova arrecadada por meio de interceptação de comunicações telemáticas exige o mesmo nível de cuidado em sua cadeia de custódia, pois veja-se que, tal qual os vestígios de um local de crime ou de amostras médico-legais, ela será igualmente única e irrepetível, devendo, por tal razão, ser preservada em sua inteireza, em sua forma autêntica e genuína, para, posteriormente, ser amplamente disponibilizada às partes até o término do processo penal ou até sua regular destruição.

Daí a relevância de se definir o que seria uma regular destruição.

No sistema italiano, existem dispositivos legais voltados para a preservação da prova de comunicações e para assegurar o direito das partes de apontar, elas próprias, em quais pontos do material amealhado reside seu interesse probatório[659]. Paolo Tonini (2002) observou que o desentranhamento e a posterior destruição do material inútil podem ser requeridos pelas partes ou determinados de ofício pelo juiz, que deverá permitir a manifestação das partes, ou seja, o juiz é levado a introduzir no processo todas as gravações porque a lei lhe permite desentranhar e destruir somente os atos indubitavelmente irrelevantes e após ter comunicado as partes[660].

Indo além, o italiano Alberto Camon observa o inconveniente de que essa fase de seleção do material de interesse das partes ocorra antes que a acusação tenha sido formulada, pois a prerrogativa das partes de indicarem o que efetivamente lhes será pertinente fica dificultada quando exercida antes da apresentação de uma imputação[661].

Na Espanha, o legislador se preocupou com a adequada conservação da prova obtida por meio de interceptação de comunicações. Está no artigo 97 do *Real Decreto* 424/2005, que impõe a adoção de "*todos los medios necesarios para impedir la manipulación de los mecanismos de interceptación, y para garantizar la autenticidad, confidencialidad e integridad de la información obtenida con la interceptación*"[662].

Também quanto aos dados de tráfego[663], a lei espanhola preocupou-se em impedir sua manipulação, destruição acidental ou ilícita ou sua perda acidental, tendo determinado a adoção de medidas técnicas para tanto[664].

---

[659] TONINI, 2002, p. 251/252.
[660] Ibid., p. 252.
[661] Em razão disso, o autor sugere que a seleção das comunicações relevantes seja feita depois do pedido de "*rinvio a giudizio*" e antes da audiência preliminar (CALMON, Alberto. **Le intercettazioni nel processo penale**. Milano: Giuffrè, 1996, p. 222/223).
[662] Ver item 3.3.2, *supra*.
[663] Ver no item 4.11 a distinção entre dados de tráfego e dados de conteúdo, bem como a distinção ao tratamento de um e de outro.
[664] Ver item 3.3.3.

Por outro lado, a *Ley Orgánica* 2/2002, da Espanha, em seu artigo único, inciso 4, dispõe que o Secretário de Estado Diretor do *Centro Nacional de Inteligencia* ordenará "*la inmediata destrucción del material relativo a todas aquellas informaciones que, obtenidas mediante la autorización prevista en este artículo, no guarden relación con el objeto o fines de la misma*"[665], abrindo a possibilidade de supressão de material probatório sem que haja na lei dispositivo voltado para assegurar a fiscalização da medida ou participação da defesa.

A esse respeito, o espanhol Juan Montero Aroca (1999) assinalou a necessidade de que a seleção do material seja realizada pelo juiz e com audiência das partes, tendo em vista que só elas próprias poderiam apontar em quais comunicações, dentre as captadas, têm interesse, não se podendo privá-las de possíveis fontes de prova a serem utilizadas no *juicio oral*[666].

Voltando ao Brasil, conquanto a disposição do parágrafo único do artigo 9º da Lei 9.296/96 não seja suficientemente clara, a necessidade de obediência ao contraditório e à ampla defesa nessa fase decorre diretamente do texto constitucional, mostrando-se evidente que o incidente de inutilização deve ser necessariamente realizado na presença do acusado e de seu defensor, até porque se trata de momento do procedimento probatório em que se faz a seleção das provas pertinentes e relevantes para o julgamento[667].

O Projeto de Código de Processo Penal traz um aspecto positivo quanto a essa problemática, dispondo, em seu artigo 256, §1º, que, decorridos 60 dias do encaminhamento do auto circunstanciado, o juiz, ouvidos o Ministério Público e a defesa, determinará a inutilização do material que não interessar ao processo. No parágrafo segundo, no entanto, o Projeto manteve a redação – a nosso ver inadequada – no sentido de exigir, no ato de inutilização do material, tão somente a presença do Ministério Público, e apenas facultar a presença do acusado e de seus representantes legais[668].

Veja-se, sob outro ângulo, que, no mundo atual, com a extrema popularização dos mais diversos meios de comunicação, os diálogos são fracionados por inúmeras vias

---

[665] Ver item 3.3.5.

[666] "El derecho de defensa y la contradicción, llevados ahora a la fase de instrucción, no pueden consentir que el Juez decida, sin audiencia de las partes, qué conversaciones tienen interés a los efectos del proceso penal. El Juez no pude privar a las partes, a cualquiera de ellas, de una posible fuente de prueba para el juicio oral, y lo que va ser utilizado por las partes como fuente de prueba han de poder decidirlo ellas, sin perjuicio de que el Juez incorpore a las actuaciones lo que, a su vez, estime conveniente" (AROCA. Juan Montero. **La intervención de las comunicaciones en el proceso penal**: un estudio jurisprudencial. Valencia: Tirant lo Blanch, 1999, p. 249).

[667] GRINOVER, Ada Pellegrini. Parecer juntado aos autos do HC 160.662/RJ, em trâmite no Superior Tribunal de Justiça, ainda prendente de julgamento.

[668] Art. 256. ... § 1º Decorridos 60 (sessenta) dias do encaminhamento do auto circunstanciado, o juiz, ouvidos o Ministério Público e a defesa, determinará a inutilização do material que não interessar ao processo. § 2º A inutilização do material será assistida pelo Ministério Público, sendo facultada a presença do acusado ou da parte interessada, bem como de seus representantes legais (Parecer nº 1.636, de 2010, estabelecendo a redação final do Projeto de Lei do Senado nº 156, de 2009. Disponível em: <http://www.senado.gov.br/atividade/materia/getPDF.asp?t=85509&tp=1>. Acesso em: 04 já. 2014).

comunicativas, ou seja, é comum que uma conversa que se iniciara por telefone, seja complementada por WhatsApp, mais bem esclarecida por SMS, desmentida por Skype e, por fim, retificada por e-mail.

Diante do exemplo, pode-se compreender que a indevida seleção ou a irregular destruição de parte do material comunicativo coletado pelo Estado seria causa de imprestabilidade integral do material captado, tendo em vista a quebra da cadeia de custódia, a quebra da confiabilidade do todo probatório, a não preservação da prova em sua forma inteira e genuína.

Não é que uma prova obtida em interceptação de comunicações só tenha valor se englobar todas as formas comunicativas possíveis e imagináveis que um indivíduo alvo utilize em seu dia a dia. É óbvio que haverá valor probatório na interceptação de e-mail de um indivíduo, mesmo que não se esteja captando o que ele fala, complementa, retifica ou desmente através de outras vias comunicativas. Bem diferente, no entanto, será a hipótese de se interceptar quatro formas comunicativas de um alvo, tais como telefone fixo, telefone móvel, e-mail e Skype, e, antes que a defesa possa ter acesso ao todo probatório amealhado, o juiz ou quem quer que seja decida, unilateralmente, por inutilizar o material decorrente da linha de telefone fixo porque entendeu que dela não teriam advindo diálogos relevantes.

Tal prática se mostra irrazoável até mesmo perante o senso comum, senão imaginemos a seguinte situação: numa interceptação, o Estado retira do indivíduo o direito ao sigilo sobre suas comunicações, com o que lhe invade direitos caros como os da intimidade e privacidade, tudo em nome do interesse da comunidade. Depois, na fase judicial, quando ao réu restaria apenas o contraditório diferido, postergado e, portanto, menos efetivo do que o contraditório pleno, ele descobre que, meses antes de sua "chegada" aos autos, meses antes do início de sua *participação*, trechos das comunicações captadas já foram avaliadas, consideradas inúteis e irreversivelmente descartadas.

Em tal hipótese, portanto, a destruição de parte da prova ou mesmo a inobservância, dolosa ou culposa, de uma cadeia de custódia capaz de assegurar a integridade, a confiabilidade, a unicidade e a originalidade da prova a inquinaria de ilícita e inservível.

Isto porque, evidentemente, ninguém pode substituir a própria defesa na verificação do que constitui ou não elemento de seu interesse. A destruição de um trecho que seria de interesse da defesa (que só por ela poderá ser apontado) invalida a integralidade do material captado na interceptação.

Fazendo-se, por fim, uma comparação entre as normas que cercam a inutilização de comunicações inservíveis na Itália e no Brasil, é possível afirmar que o ordenamento do

primeiro país se aproxima mais do ponto de equilíbrio tido como meta de eficiência e garantismo do que o do Brasil, porquanto, neste último, a possibilidade sinalizada pela lei de que se suprimam irreversivelmente fontes de prova, sem que a defesa possa antes avaliar se delas irá se servir, impede que um dos sujeitos processuais, mais precisamente o acusado, exerça adequadamente suas faculdades, seus direitos, suas garantias, porquanto lhe suprime o direito à prova, violando a ampla defesa e o contraditório, ambos integrantes do núcleo essencial de garantias, pelo que se inviabiliza a incidência real das normas de garantia.

4.8 Acesso ao material captado

Sabe-se que a medida de interceptação de comunicações depende, como um de seus requisitos mais elementares, de um sigilo a ser oponível a todos os investigados, sob pena de se frustrar a colheita da prova.

Por isso, em caso de inquérito cuja existência já seja de conhecimento do suspeito ou de seu advogado, eventual interceptação que esteja em andamento terá de tramitar em autos apartados, de modo a se preservar o sigilo das diligências, gravações e transcrições respectivas (art. 8º da Lei 9.296/96).

Tal sigilo deverá perdurar enquanto a medida estiver em andamento, não havendo qualquer sentido, no entanto, em mantê-lo oponível ao suspeito depois de concluída a medida.

Observa Lenio Streck (2001) que, evidentemente, não pode o réu ou investigado ter ciência da interceptação em andamento ou a se iniciar, mas, após concluída a captação, deve-lhe ser assegurado acesso a seu conteúdo através de seu defensor constituído[669].

Menos sentido ainda faria manter o sigilo depois de posta a acusação, pois, nas palavras de Antonio Scarance Fernandes, as partes devem logo ter acesso ao material obtido com a interceptação, o Ministério Público para embasar a acusação e o acusado para responder à acusação[670].

Vicente Greco Filho (1996) fala em acesso pelo réu ou investigado ao material captado na interceptação "na primeira oportunidade que houver após sua realização"[671].

---

[669] STRECK, 2001, p. 100.
[670] FERNANDES, 2010, p. 100.
[671] GRECO FILHO, 1996, p. 37.

Raúl Cervini e Luiz Flavio Gomes (1997) entendem que o direito de acesso pelo investigado ou réu ao material captado se inicia quando concluídas as diligências, gravações e transcrições. Observam que, diferentemente de outros ordenamentos, o brasileiro não previu o dever do Estado de, uma vez concluídas as diligências, notificar o investigado e terceiros interlocutores, de modo a permitir-lhes conhecer o que fora captado a seu respeito e a exercer, com maior liberdade, a ampla defesa, mas, apesar de não expressamente previsto, afirmam que o resultado final não poderia ser diferente[672].

Ao editar a Súmula Vinculante nº 14[673], atinente ao direito que o investigado tem de acessar autos de inquérito que tramite em seu desfavor, o STF restringiu tal acesso àqueles elementos "já documentados em procedimento investigatório", de modo a que não se interprete o verbete como forma de assegurar ao requerido a ciência de cautelares *inaudita altera pars* pendentes de cumprimento, tais como busca e apreensão, prisão cautelar e interceptação de comunicações.

Cumpre observar que, embora pareça tão elementar e essencial, os Estados Unidos, como retratado nos itens 3.1.5 e 3.1.7, não asseguram ao réu um amplo direito de acesso ao material captado em interceptações. Muito pelo contrário, a *Section* 2518(8)(d) do *Title* 18 do USC dispõe que o juiz, quando provocado, poderá, conforme sua discricionariedade, disponibilizar à pessoa interceptada ou a seu advogado, para inspeção, os trechos das comunicações interceptadas, pedidos e decisões que ele juiz determinar que sejam do interesse da justiça.

Até mesmo diante de pedido do réu no sentido de que comunicações colhidas sejam suprimidas em razão de ilicitude de alguma natureza, tudo que a *Section* 2518(10)(a)(iii) prevê em termos de acesso defensivo é, no mesmo sentido da *Section* 2518(8)(d), que o juiz *poderá, dentro de sua discricionariedade*, disponibilizar à pessoa prejudicada pela prova ilícita ou ao seu advogado, para inspeção, partes da interceptação ou prova dela derivada que ele juiz determine ser do interesse da justiça[674].

Além de, novamente aqui, tratar-se de alguém (no caso, o juiz) a se substituir às partes na identificação dos elementos que sejam ou não de seu interesse probatório, ou "do interesse da justiça", vê-se que inexiste no ordenamento norte-americano um direito automático da

---

[672] GOMES; CERVINI, 1997, p. 229/231.

[673] "É direito do defensor, no interesse do representado, ter acesso amplo aos elementos de prova que, já documentados em procedimento investigatório realizado por órgão com competência de polícia judiciária, digam respeito ao exercício do direito de defesa." (BRASIL. Supremo Tribunal Federal. Súmula Vinculante nº 14. Pleno. Aprovada na sessão de 02.02.2009).

[674] Ver, no item 3.1.7, o precedente *United States v. Appelbaum*, a *United States Court of Appeals for the Fourth Circuit* no qual foi mantida a decisão recorrida de impedir o acesso do defensor às ordens judiciais que requisitaram conteúdo de comunicações eletrônicas armazenadas, mesmo já estando inaugurada a fase judicial.

defesa de ter ciência e fiscalizar, ainda que *a posteriori*, o desenvolvimento da interceptação e sua obediência às prescrições legais e aos prazos. Inexiste, enfim, uma liberdade da defesa de compulsar a integralidade do que foi captado para só então verificar onde reside seu interesse probatório.

Não se tem dúvida, portanto, em concluir que, quanto ao direito de acesso ao material captado por meio das interceptações, o ordenamento brasileiro permite o exercício das prerrogativas processuais das partes muito melhor do que o norte-americano, pelo que se pode classificá-lo de mais eficiente e assegurador do núcleo essencial de garantias, especificamente quanto ao contraditório e à ampla defesa.

4.9 Prova ilícita

O estudo da interceptação das comunicações telemáticas, tal qual o das telefônicas, se vincula intimamente ao tema da ilicitude de prova, tendo em vista que a invasão indevida na intimidade e na privacidade do indivíduo, sem obediência às estritas exigências constitucionais e legais, grava de ilícita a prova arrecadada.

A doutrina nacional tem empregado a distinção proposta por Ada Pellegrini Grinover que, com base em Pietro Nuvolone, diferencia a prova ilícita da prova ilegítima, afirmando que a primeira ocorre quando a proibição violada for de natureza material, ao passo que a segunda se dá quando a proibição for colocada por uma lei processual. Ambas as espécies pertenceriam ao gênero das provas ilegais[675].

A reforma processual penal de 2008, no entanto, mais precisamente a alteração implementada pela Lei 11.690/08, retirou a importância da distinção na medida em que destinou tratamento idêntico às duas espécies de provas ilegais. Nesse sentido, o artigo 157 do CPP prescreveu que "são inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas constitucionais ou legais".

A norma acima foi criticada[676] em razão de sugerir que não mais haveria diferença entre a sanção processual a ser aplicada às provas ilícitas (não ingresso no processo ou

[675] GRINOVER, 1996, p. 48.
[676] GRINOVER; GOMES FILHO; FERNANDES, 2009, p. 125; GOMES FILHO, Antonio Magalhães. Provas: Lei 11.690, de 09.06.2008 In: MOURA, Maria Thereza Rocha de (Coord.). **As reformas no processo penal**: as novas leis de 2008 e os projetos de reforma, p. 246/297, São Paulo, Revista dos Tribunais, 2008, p. 266.

desentranhamento, caso já tenha ingressado) e aquela a ser aplicada às ilegítimas (nulidade, passível de renovação, na forma do art. 573 do CPP[677]).

Gustavo Badaró observou, todavia, que, muito embora no campo abstrato seja clara a distinção entre prova ilícita e prova ilegítima, o mesmo não se dá no campo prático, tendo em vista que uma mesma ilegalidade pode, muito comumente, ter aspecto bifronte, ou seja, violar dispositivos constitucionais ou legais que podem ser lidos, tanto como uma norma de proteção a liberdades públicas, quanto como um regramento processual delimitando mecanismos para realização de um meio de prova ou de obtenção de prova[678]. Ademais, a distinção entre violação de norma de direito processual e violação de norma de direito material não seria uma constante em direito comparado, propondo o autor, ao fim, a definição de prova ilícita como aquela obtida, admitida ou produzida com violação das garantias constitucionais, sejam as que asseguram liberdades públicas, sejam as que estabelecem garantias processuais[679]. O desentranhamento se constituiria em mero mecanismo técnico para assegurar uma proibição de valoração dessa prova ilícita[680]. Também no que diz respeito à prova ilícita por derivação, a visão proposta por Gustavo Badaró não alteraria o resultado a que se chegaria, quer fosse a prova originária ilícita, quer fosse ilegítima, pois o mesmo nexo causal exigido entre prova ilícita originária e derivada precisa se fazer presente na aplicação da teoria das nulidades (art. 573, §1º, CPP[681])[682].

Filiamo-nos a este último entendimento, que, nas palavras do autor, veio, não a negar a doutrina clássica formada a partir da posição da Professora Ada Pellegrini Grinover, mas a ampliar seu campo de incidência, buscando um conceito operacionalmente mais útil para a finalidade de garantir o respeito às garantias constitucionais que asseguram direitos fundamentais, sejam de conteúdo material, sejam de natureza processual[683].

O item 3.1.7, *supra*, retratou os dispositivos da legislação dos Estados Unidos sobre a inadmissibilidade do produto de interceptação ilícita de comunicações eletrônicas, tendo aquele país, no *Title* 18, *Section* 2518 do USC, previsto um remédio do qual qualquer pessoa prejudicada poderá lançar mão no sentido de buscar a supressão do material reputado ilícito, sempre que este houver sido colhido ilegalmente ou quando a decisão que houver autorizado a

---

[677] CPP. Art. 573. Os atos, cuja nulidade não tiver sido sanada, na forma dos artigos anteriores, serão renovados ou retificados.
[678] BADARÓ, 2012, p. 288.
[679] BADARÓ, 2012, p. 289.
[680] Ibid., p. 289.
[681] CPP. Art. 573. ... § 1º A nulidade de um ato, uma vez declarada, causará a dos atos que dele diretamente dependam ou sejam conseqüência.
[682] BADARÓ, 2012, p. 287.
[683] BADARÓ, 2012, p. 289.

medida não for suficiente ou, ainda, quando a execução da medida houver excedido os termos da autorização concedida. A petição deverá ser feita antes do julgamento, audiência ou procedimento, a menos que não haja oportunidade para fazê-lo ou caso o requerente não conheça ainda os motivos do pedido. Sendo deferido, o conteúdo da interceptação e as provas dele derivadas serão consideradas ilícitas.

Muito embora tal dispositivo legal pareça criar normas e mecanismos aparentemente eficazes, a discricionariedade excessiva dada ao Judiciário no campo da prova ilícita por derivação tem o potencial de esvaziar o próprio sentido da norma protetiva do indivíduo, como se viu no caso *Jody Lee Miles v. State of Maryland*[684]. Em tal caso, a *Court of Appeals of Maryland* não vislumbrou ilicitude por derivação na apreensão da arma e das roupas que o réu utilizou no cometimento do crime, mesmo quando tal apreensão só se deu porque a companheira do réu revelou o esconderijo à polícia enquanto tinha sua casa invadida mediante mandado de busca e apreensão que fora obtido com o uso de uma comunicação interceptada ilegalmente.

Noutras palavras, a mesma Corte que reconheceu a interceptação como ilícita afirmou que a conexão entre esta e as palavras proferidas pela companheira do réu enquanto sua casa era invadida em razão daquela interceptação seria tão tênue, que a mácula de ilicitude teria se dissipado, para o que invocou entendimento da Suprema Corte dos Estados Unidos segundo o qual testemunhas não são como armas ou documentos, que ficam escondidos da vista da polícia até alguém levantar um sofá ou abrir um armário, mas elas, ao contrário, podem oferecer provas de forma absolutamente voluntária, como frequentemente fazem[685].

A dita atenuação dos efeitos da ilicitude sobre a prova derivada se baseou no que o acórdão chamou de *Brown test*, em referência ao raciocínio adotado pela Suprema Corte no caso *Brown v. Illinois*, em que uma confissão colhida durante prisão reconhecidamente ilegal foi reputada válida pelo fato de a polícia ter promovido o chamado *Miranda warnings*, ou seja, por ter advertido o réu de seu direito de permanecer calado, tendo-se tomado em consideração na análise também outros fatores como a proximidade temporal entre o ato ilícito e a obtenção da prova derivada, bem como o propósito e a flagrância da má conduta policial[686].

No Brasil, a Constituição foi categórica e taxativa ao estabelecer, no artigo 5º, inciso LVI, a regra da inadmissibilidade das provas obtidas por meios ilícitos, sem dar margem a

---

[684] Ver item 3.1.7.
[685] Ver item 3.1.7.
[686] Abordamos a concepção norte-americana de *Brown test* no item 3.1.7.

sopesamentos de valores e aplicação do princípio da proporcionalidade para mitigá-la com base na gravidade do delito[687]. De nada adiantaria a norma constitucional, se fosse possível salvar a prova ilícita, lançando mão de interpretações tolerantes por meio de raciocínios como o *Brown test* ou afirmar que o uso do *Miranda warnings* ao final de uma sequência de atos policiais inaugurada por algum excesso policial criminoso pudesse atenuar ou dissipar a contaminação da ilicitude de origem sobre a prova derivada.

Do contrário, estar-se-ia a permitir o que se poderia chamar de uma espécie de *lavagem de prova ilícita*, expressão que usamos em alusão ao crime de lavagem de dinheiro[688], ou seja, estar-se-ia admitindo um expediente intermediário entre a ilicitude originária e a prova derivada, com fins a dissimular sua origem e dar por superada aquela ilicitude. Um método, aliás, que se popularizou para se fazer a tal lavagem de prova ilícita é o uso, por agentes do próprio Estado, de delações anônimas montadas para fazer chegar aos autos uma informação a que se teve acesso de forma ilícita. Isto, a nosso ver, ao retirar da defesa técnica a possibilidade de compreender e fiscalizar a exata origem de cada elemento probatório surgido nos autos, sua rastreabilidade, enfim, acaba por ofender o núcleo essencial de garantias[689], precisamente em seus componentes ampla defesa e contraditório, na medida em que ela não pode se fazer efetiva.

A conhecida história da evolução da prova ilícita nos Estados Unidos[690], antes admissível no processo e que ensejava tão somente a punição do agente estatal, mostrou que só os mecanismos de absoluta imprestabilidade probatória, o que – é óbvio – há que valer também para as derivadas, têm condições de efetivamente coibir as práticas ilícitas do Estado persecutor contra o indivíduo.

---

[687] BRASIL. Supremo Tribunal Federal. HC 80949/RJ, rel. min. Sepúlveda Pertence, 1ª T., j. 30.10.2001, DJ 14.12.2001: "Guarda da Constituição – e não dos presídios – é dessa opção clara, inequívoca, eloqüente da Constituição – da fidelidade à qual advém a nossa própria legitimidade – é que há de partir o Supremo Tribunal Federal. Ora, até onde vá a definição constitucional da supremacia dos direitos fundamentais, violados pela obtenção da prova ilícita, sobre o interesse da busca da verdade real no processo, não há que apelar para o princípio da proporcionalidade, que, ao contrário, pressupõe a necessidade da ponderação de garantias constitucionais em aparente conflito, precisamente quando, entre elas, a Constituição não haja feito um juízo explícito de prevalência. ... Certo, a Constituição reservou a determinados crimes particular severidade repressiva (Art. 5º, XLII, XLIII e XLIV). Mas, como observa Magalhães Gomes Filho, por sua natureza, as restrições que estabelecem são taxativas: delas, não se podem inferir, portanto, exceções a garantia constitucional – qual, a da vedação da prova ilícita –, estabelecida sem limitações em função da gravidade do crime investigado. ... Abstraio-me, por conseguinte, no caso, de qualquer consideração da extrema gravidade dos delitos, da participação nos quais é suspeito o paciente, pois delas não pode resultar emprestar-se menor peso à vedação constitucional da prova ilícita."

[688] Lei 9.613/98: Art. 1º Ocultar ou dissimular a natureza, origem, localização, disposição, movimentação ou propriedade de bens, direitos ou valores provenientes, direta ou indiretamente, de infração penal. (Redação dada pela Lei nº 12.683, de 2012)

[689] Sobre o conceito de núcleo essencial de garantia, ver item 1.4.

[690] GOMES FILHO, 2008, p. 262/263.

Uma vez se assumindo que a reunião de elementos probatórios ilícitos há que ser coibida, e diante da amplitude da discricionariedade que se pode construir com os mais criativos raciocínios judiciais em torno da aplicação da *inevitable discovery* e *independent source*[691], entendemos que, em matéria de exame de ilicitude por derivação, a regra deve ser a de que uma ilicitude no curso da investigação contamine todas as provas subsequentes, devendo o aproveitamento destas residir no campo da excepcionalidade.

Nesse sentido, se, por um lado, criticamos, no item 4.3, as tentativas vãs de sistematizar ou criar microssistemas normatizadores da valoração de juízo de probabilidade ou verossimilhança e mesmo do dito juízo de certeza necessário para provimentos judiciais finais, já que a palavra final do raciocínio sempre acabará entregue à incontrolável discricionariedade humana, por outro, entendemos que a análise da ilicitude por derivação pode e deve ser eminentemente objetiva e que o pouco que sobra neste campo para a discricionariedade humana quanto ao exame da relação de causalidade entre a prova ilícita originária e a prova ilícita por derivação deve ter interpretação restritíssima em favor do indivíduo. Do contrário, estar-se-ia adotando postura tolerante em relação a *pequenas ilicitudes* cometidas no ato de se violar o sigilo das comunicações e, junto com ele, a intimidade e a privacidade do indivíduo, gerando verdadeiro retrocesso no caminho já percorrido no sentido de conter os abusos do Estado nesta área.

A título de exemplo, se, durante a interceptação da conta de e-mail de Tício, que tenha contado com sucessivas renovações, restou excedido, numa delas, o período de 15 dias, tendo-se captado suas mensagens por dois dias além do período autorizado, a busca e apreensão deferida posteriormente pelo magistrado deverá ser reputada ilícita por derivação em relação a Tício. Se comunicações ilicitamente captadas integravam os autos no momento da apreciação judicial da representação pelas buscas e apreensões, impossível será se precisar se elas exerceram ou não alguma influência no convencimento do juiz e, nesse caso, a regra deve ser a de que houve contaminação pela prova ilícita.

A constatação é, a nosso ver, objetiva. Servindo-nos ainda do mesmo exemplo acima, temos que, quanto a uma busca e apreensão deferida no mesmo momento contra corréus ou co-investigados de Tício, entendemos que a verificação ganha, aí sim, algum nível de subjetividade, porém, ao menor sinal de que as comunicações de Tício naqueles dois dias não contemplados pela autorização possam ter gerado qualquer influência no convencimento do

[691] Os conceitos de *inevitable discovery* (descoberta inevitável) e *independent source* (fonte independente) foram positivados na legislação brasileira pela Lei 11.690/2008, que alterou a redação do artigo 157 do CPP.

magistrado em relação à busca e apreensão deferida contra os demais, é de reconhecer, como regra, a ilicitude por derivação também em relação a eles.

Noutro exemplo, se a polícia lança mão de um *hacker* para, sem ordem judicial, invadir e espelhar a conta de *Skype* de um investigado, reproduzindo para o investigador tudo quanto ele fala, ouve, lê e escreve, e, com base nisso, obtém-se ordem de prisão temporária em cuja execução se extrai uma confissão com a qual se deflagra uma ação penal, o caso será de ilicitude da ação *ab initio*, de imprestabilidade desde seu nascedouro, não havendo razoabilidade em se afirmar que, só porque ele fora advertido quanto ao direito ao silêncio ou pelo fato de que pessoas, diferentemente de objetos escondidos num armário ou sob um sofá, podem falar voluntariamente, a ilicitude por derivação tenha-se dissipado.

Vale observar que o sistema inglês, quanto a este ponto, traz peculiaridades como a existência de um tribunal especializado em avaliar a licitude de uma interceptação, o *Investigatory Powers Tribunal*, cujas decisões são soberanas, não podendo ser reformadas nem pela Suprema Corte do país[692]. Será a partir de uma decisão deste Tribunal que, uma vez reconhecida a ilicitude, se procederá à destruição do material captado. Mas, se o Estado inglês deu com uma mão, tirou com a outra, pois, em primeiro lugar, há registros de que, das 956 interceptações que tiveram sua licitude analisada pelo referido Tribunal num período de nove anos, somente quatro foram consideradas ilegais e, em segundo lugar, a mesma legislação que estabeleceu a inadmissibilidade probatória do material interceptado ilicitamente trouxe um extenso rol de exceções, não à ilicitude, mas à inadmissibilidade. Nesse sentido, a *Section* 18 do RIPA prevê que, não obstante tenha sido ilicitamente arrecadada, a prova poderá ser usada num sem número de situações, especialmente nas relativas a casos de terrorismo e organizações proibidas[693].

Podemos dizer, portanto, que, quanto ao tema atinente ao tratamento da prova ilícita, a legislação brasileira seguiu mais os parâmetros de eficiência e garantismo, se aproximando mais da meta de ponto médio entre hipergarantismo e repressão a todo custo do que a Inglaterra. Quanto aos Estados Unidos, temos que sua legislação contém dispositivos de aparente eficácia, mas que acabam esvaziados em razão da ampla discricionariedade dada aos tribunais no tratamento da ilicitude por derivação, que, a nosso ver, há que ser objetivo e deve ter a inadmissibilidade probatória como regra e o aproveitamento como rara exceção.

---

[692] Ver item 3.2.5.
[693] Ver item 3.2.4.

4.10 Encontro fortuito de provas

A doutrina costuma distinguir dois conceitos, o de *conhecimentos de investigação* e o de *conhecimentos fortuitos*.

Os primeiros são os fatos obtidos através de uma interceptação legalmente efetuada, que se refiram ao crime objeto da investigação que ensejou a autorização da medida ou a outro delito (pertencente ou não ao catálogo legal) que esteja baseado na mesma situação histórica da vida daquele. Já os conhecimentos fortuitos são definidos como aqueles fatos ou conhecimentos obtidos através de uma interceptação legalmente efetuada, mas que não tenham relação, nem com o crime cuja investigação determinou a realização da medida, nem com qualquer outro delito (pertencente ou não ao catálogo legal) que esteja baseado na mesma situação histórica da vida daquele[694].

Mais complexa, no entanto, do que a mera definição do que vem a ser conhecimento fortuito será a verificação da validade da prova encontrada fortuitamente numa interceptação.

No direito alemão, a prova assim alcançada tem valor jurídico, desde que o fato encontrado fortuitamente tenha conexão com algum dos crimes que autorizam a interceptação, ou seja, não se exige conexão com o crime investigado no caso concreto, mas apenas com algum dos crimes constantes do rol previsto na lei[695].

Na Itália, conforme se extrai do artigo 270 do CPP italiano[696], os resultados das interceptações são utilizáveis como prova, em regra, somente no âmbito do procedimento em que a medida houver sido determinada, podendo ser utilizados noutros procedimentos quando forem indispensáveis para a averiguação de delitos para os quais seja obrigatória prisão em

---

[694] AGUILAR, Francisco. **Dos conhecimentos fortuitos obtidos através de escutas telefônicas**. Coimbra: Almedina, 2004, p. 17/18. Para Manuel da Costa Andrade, conhecimentos de investigação seriam os fatos apurados numa interceptação que tenham relação com os crimes que são diretamente objeto da investigação e que ensejaram o deferimento da medida, enquanto conhecimentos fortuitos se refeririam a outros crimes verificados na comunicação captada (ANDRADE, Manuel da Costa. Das escutas telefônicas. In: SILVA, Marco Antonio da (Coord.). **Direito penal especial, processo penal e direitos fundamentais**: visão luso-brasileira. São Paulo: Quartier Latin do Brasil, 2006, p. 205/213).

[695] GOMES, Luiz Flavio. Interceptação telefônica e "encontro fortuito" de outros fatos. **Boletim do Instituto Brasileiro de Ciências Criminais**, São Paulo, n. 51, fev. 1997, p. 6.

[696] TITOLO III - Mezzi di ricerca della prova. Capo IV - Intercettazioni di conversazioni o comunicazioni. Articolo 270 - Utilizzazione in altri procedimenti. 1. I risultati delle intercettazioni non possono essere utilizzati in procedimenti diversi da quelli nei quali sono stati disposti, salvo che risultino indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza (380). 2. Ai fini della utilizzazione prevista dal comma 1, i verbali e le registrazioni delle intercettazioni sono depositati presso l'autorità competente per il diverso procedimento. Si applicano le disposizioni dell'articolo 268 commi 6, 7 e 8. 3. Il pubblico ministero (51) e i difensori (96 ss.) delle parti hanno altresì facoltà di esaminare i verbali e le registrazioni in precedenza depositati nel procedimento in cui le intercettazioni furono autorizzate. Disponível em: <http://www.diritto.it/codici/articolo/4315466-codice-di-procedura-penale-utilizzazione-in-altri-procedimenti>. Acesso em: 05 jan. 2014.

flagrante[697]. Fora destas hipóteses, segundo Paolo Tonini (2002), as provas fortuitamente encontradas permanecem utilizáveis como *notitia criminis* para outros procedimentos[698].

Nos Estados Unidos, conforme abordado no item 3.1.8, há dispositivo legal específico sobre o tratamento a ser destinado a provas fortuitamente encontradas em interceptações. Diz o *Title* 18, *Section* 2517(5) do USC que, sempre que forem encontradas provas de crimes outros que não aqueles especificados na autorização ou aprovação[699], estas poderão ser encaminhadas para a apuração própria, mediante concordância do juiz com a legalidade da interceptação que as captou.

Já se o material revelar informações de inteligência ou contrainteligência estrangeira ou ameaça de ataque ou hostilidade de poder estrangeiro, sabotagem doméstica ou internacional, terrorismo doméstico ou internacional ou, ainda, atividades de reuniões clandestinas de serviços de inteligência ou de rede de poderes estrangeiros, qualquer oficial de investigação ou procurador poderá, independentemente de intervenção judicial, divulgá-lo para qualquer outro oficial de aplicação da lei, inteligência, proteção, imigração, defesa nacional ou segurança nacional[700].

Ou seja, o sistema norte-americano se limita a fazer – e, mesmo assim, somente em algumas hipóteses – um juízo acerca da legalidade da interceptação originariamente deferida, sem qualquer consideração sobre a gravidade dos fatos encontrados fortuitamente ou sobre sua conexão com o fato que deu causa à medida.

Antonio Scarance Fernandes (2010) chama de problema difícil o surgimento de prova relativa a crime diverso daquele para o qual a medida foi autorizada e o compara com o surgimento, numa busca e apreensão, de objeto diverso daquele procurado, mas relevante para a prova do crime apurado ou de outro delito. Sustenta que, em princípio, haverá ilicitude por desvio do objeto da interceptação ou da busca, mas que nem sempre tal desvio de objeto gerará ilicitude e inadmissibilidade da prova, devendo-se adotar o critério do nexo entre o crime descoberto e o crime investigado[701].

Vicente Greco Filho (1996) entende possível o uso de prova encontrada fortuitamente caso se refira à infração penal que também seja passível de interceptação e que tenha relação

---

[697] TONINI, 2002, p. 252.
[698] Ibid., p. 252.
[699] O instituto da *approval* judicial de uma interceptação promovida sem ordem judicial foi objeto de abordagem no item 3.1.6.
[700] *Title* 18, *Section* 2517(6) e (8) do USC.
[701] FERNANDES, 2010, p. 98.

com o crime que deu origem à medida, com ele ensejando concurso de crimes, continência ou conexão[702].

Raúl Cervini e Luiz Flavio Gomes (1997) observam que o que se espera sempre é a identidade ou a congruência entre o fato e o sujeito indicados na decisão e o fato e o sujeito efetivamente investigados ou descobertos. Havendo discordância, sustentam que se deve comunicar tudo imediatamente ao juiz pelo princípio do controle judicial, para que ele decida a respeito, apontando como fundamental o critério da conexão, segundo o qual se deve delimitar o grau de conexão necessário para que a prova seja admitida como válida. Nesse sentido, entende válida a prova se se descobre fato delitivo conexo com o fato investigado, desde que seja de responsabilidade do mesmo sujeito passivo. Não atendida tal exigência, o elemento colhido fortuitamente valeria apenas como fonte de prova, a partir da qual se poderia desenvolver nova investigação[703].

Para Lenio Streck (2001), em se tratando de crime grave, que se enquadre no que chamou de reserva constitucional passível de interceptação, não poderá o Estado ignorar dado revelador de tal crime, mesmo sendo diverso daquele para o qual a medida foi autorizada. Por outro lado, sustenta que o dado surgido não poderá ser usado como prova bastante para a instauração de uma ação penal, mas sim servir de indício para a busca (uma nova busca) da comprovação da existência do crime[704].

Na visão de Ada Pellegrini Grinover, Antonio Magalhães Gomes Filho e Antonio Scarance Fernandes (2009), a falta de um rol taxativo de infrações em que se admite a interceptação dificulta a solução do problema, podendo o juiz, no entanto, guiar-se pelo critério de gravidade do crime de forma análoga ao que se faz em ordenamentos estrangeiros, tal qual os autores propuseram em relação ao próprio cabimento da interceptação originária (art. 2º, III da Lei 9.296/96), que deverá ser avaliado à luz do princípio da proporcionalidade. Quanto ao surgimento de elementos de prova contra pessoas distintas dos investigados mencionados na decisão, os autores entendem que os elementos fortuitamente encontrados devem ser admitidos desde que ligados ao fato que está sendo investigado, até porque o parágrafo único do artigo 2º admite a autorização mesmo nos casos em que não tenha sido possível a indicação e a qualificação prévias dos investigados[705].

Diante da já antiga celeuma, o Projeto do Código de Processo Penal, em seu artigo 262, traz previsão de que "na hipótese de a interceptação das comunicações telefônicas

[702] GRECO FILHO, 1996, p. 21.
[703] GOMES; CERVINI, 1997, p. 192/194.
[704] STRECK, 2001, p. 129/130.
[705] GRINOVER; GOMES FILHO; FERNANDES, 2009, p. 175/176.

revelar indícios de crime diverso daquele para o qual a autorização foi dada e que não lhe seja conexo, o delegado de polícia deverá remeter ao Ministério Público os documentos necessários para as providências cabíveis"[706].

Esse ponto do Projeto, no entanto, mereceu crítica formulada pelo IBDP, que, por sua vez, propôs redação prevendo que, no caso de surgir prova de crime não contemplado no catálogo (este também proposto pelo Instituto), o juiz deverá encaminhar prova fortuitamente encontrada ao Ministério Público, que poderá requisitar a instauração de inquérito[707].

A nosso ver, há um aspecto elementar, que devemos destacar, em torno das provas fortuitamente encontradas em interceptações de comunicações.

No item 4.9, *supra*, expusemos os fundamentos pelos quais nos filiamos ao entendimento de Gustavo Badaró, no sentido de que prova ilícita é aquela obtida, admitida ou produzida com violação das garantias constitucionais, sejam as que asseguram liberdades públicas, sejam as que estabelecem garantias processuais.

Se, em matéria de interceptação de comunicações, o bem jurídico em jogo será o direito à inviolabilidade do sigilo das comunicações e, junto com ele, da intimidade e da privacidade das pessoas monitoradas, todos direitos constitucionais fundamentais protetores de liberdades públicas, está claro que eles não podem sofrer restrição indevida, ilegal ou desproporcional, sob pena de inquinar de ilícita a prova decorrente da referida violação. Neste campo, portanto, ou a prova será lícita, e aí com plena condição de gerar efeitos, ou será ilícita e, nesse caso, absolutamente inadmissível para qualquer fim.

Diante disso, não nos parece adequado o tratamento dualista da prova fortuitamente encontrada, como Paolo Tonini afirmou ocorrer[708] na Itália e como, no Brasil, defendem Luiz Flavio Gomes e Lenio Streck. É que ou ela será lícita, podendo gerar efeitos jurídicos, ou ilícita e, nesse caso, não há que ser admitida para nenhum fim, nem como notícia de crime e nem como fonte de prova para nova investigação, sob pena de se estar concebendo um

---

[706] Parecer nº 1.636, de 2010, estabelecendo a redação final do Projeto de Lei do Senado nº 156, de 2009. Disponível em: <http://www.senado.gov.br/atividade/materia/getPDF.asp?t=85509&tp=1>. Acesso em: 05 jan. 2014.

[707] Redação proposta pelo IBDP: Art. 252. Na hipótese de a quebra do sigilo das comunicações telefônicas de qualquer natureza revelar, fortuitamente, indícios de crime que não se inclua nas hipóteses do artigo 241, o juiz deverá remeter ao Ministério Público, que poderá requisitar a instauração de inquérito policial (Instituto Brasilero de Direito Processual (IBDP). Propostas de emendas ao Projeto de Lei de Código de Processo Penal. Substitutivo CCJ do Senado. Disponível em: <http://www.direitoprocessual.org.br/download.php?f=9546b22fe462eb3d2116f6ff5b62a312>. Acesso em: 05 jan. 2014).

[708] Usamos aqui a expressão "afirmou ocorrer" porque, apesar das palavras do autor (TONINI, 2002, p. 252), não pudemos extrair da leitura do art. 270 do CPP italiano que a prova encontrada fortuitamente que seja inadmissível possa ser utilizada como *notitia criminis*.

raciocínio contraditório e frontalmente violador da vedação constitucional às provas ilícitas (art. 5º, LVI) e até mesmo do artigo 157 do CPP.

Dito isto, resta definir o que tornará a prova fortuitamente encontrada lícita e admissível e o que, ao contrário, torna-la-á ilícita e inadmissível.

Na linha do que decidiram as cortes internacionais nos precedentes citados no item 1.3, eventual medida que afaste o sigilo das comunicações dos indivíduos precisa estar expressamente prevista na lei interna do Estado-Parte, em norma acessível a todos, mediante os meios de publicação, norma esta que deverá prever com clareza e precisão as condições pelas quais os poderes públicos estarão autorizados a adotar a medida de interceptação. Tais exigências se prestam a dar ao indivíduo a previsibilidade das consequências da lei e também de seus próprios atos.

Importando agora o conceito norte-americano de *expectation of privacy*, que já sustentamos ser plenamente válido para raciocinar o sistema brasileiro, e tomando em conta também o critério norte-americana denominado *Katz test*[709], podemos dizer que, ao manter comunicações com um interlocutor de sua escolha, a expectativa de privacidade do indivíduo (cuja existência é inegável) só poderá ser frustrada pelo Estado para amealhar elementos probatórios relativos àqueles crimes em relação aos quais a lei, clara, pública, acessível e prévia, admita interceptação, sob pena de faltar a necessária previsibilidade ao indivíduo e, assim, ser a interferência estatal ilegítima, porquanto reprovada no *Katz test*.

A nosso ver, portanto, a prova fortuitamente encontrada por meio de interceptação só terá validade se o crime que ela revelar for daqueles que admita interceptação, independentemente de nexo causal ou de conexão com o crime que ensejou a medida. Caso não reste atendido esse pressuposto, a prova não poderá ser utilizada para nenhuma finalidade, nem mesmo como notícia de crime ou fonte de prova para nova investigação.

No que se refere a encontro fortuito, há uma modalidade comunicativa realizada por meio de internet, a dos grupos de bate-papo (os *chats*), que gera uma peculiar situação, qual seja, a de uma autorização de monitoramento implementada num momento em que já haja registros de diversas comunicações pretéritas travadas naquele mesmo veículo de comunicação. A nosso ver, o caso constitui exemplo clássico de encontro fortuito de provas, mas aqui somos obrigados a adotar solução diversa daquela que adotamos acima, de modo a atender ao subprincípio da exigibilidade temporal. Nesse sentido, entendemos que, se uma

[709] Sobre o *Katz test*, ver item 3.1.1. Utilizado pela jurisprudência norte-americana a partir do caso *Katz v. United States* (389 U.S. 347. p. 739-741), o chamado *Katz test* se presta a responder se, sob determinadas circunstâncias, a *expectation of privacy* de um indivíduo seria ou não legítima e se, por outro lado, a sociedade estaria ou não preparada para reconhecer aquela expectativa como razoável.

interceptação das comunicações realizadas num *chat* foi regularmente autorizada em determinado dia, para perdurar por prazo determinado, com data de início bem definida, os registros de diálogos pretéritos não poderão ser aproveitados para nenhuma finalidade, sob pena de a de interceptação se transfigurar numa violação ao direito ao sigilo das comunicações sem nenhum limite de tempo.

4.11 A distinção no tratamento dos dados de tráfego e dos dados de conteúdo

As discussões existentes em torno do tratamento que deve ser dispensado aos dados de tráfego de comunicações, também chamados de dados externos às comunicações, tocam em questões como saber se estão ou não inseridos no âmbito de proteção do direito à inviolabilidade do sigilo das comunicações; se os órgãos de persecução podem acessá-los sem ordem judicial; se o nível de proteção que merecem seria igual ou inferior àquele incidente sobre o conteúdo das comunicações; e o que exatamente, dentre as tantas informações que podem existir em bancos de dados de provedores e empresas de comunicações, enquadrar-se-ia no conceito de dados de tráfego.

Pode-se dizer que há praticamente um consenso na doutrina no sentido de que o inciso XII do artigo 5º da CF, bem como a Lei 9.296/96, não abarcam o sigilo de dados que repousem em servidores, *hard disks*, sistemas de instituições bancárias, mas apenas a comunicação envolvendo esses dados[710].

Para Gustavo Badaró (2010), no caso dos dados armazenados, tal qual o que ocorre com as informações bancárias e fiscais, o sigilo sobre eles se sujeitaria à garantia geral[711] da intimidade e da vida privada (art. 5º, X, CF)[712], inclusive no que se refere aos dados armazenados relativos às próprias ligações telefônicas, ou seja, os registros de horários de chamadas, sua duração, número de origem e número do destinatário não seriam protegidos

[710] MENDES; COELHO; BRANCO, 2008, p. 392: "Para o STF, ademais, o sigilo garantido pelo art. 5º, XII, da CF refere-se apenas à comunicação de dados, e não aos dados em si mesmos. A apreensão de um computador, para dele se extraírem informações gravadas no hard disk, por exemplo, não constitui hipótese abrangida pelo âmbito normativo daquela garantia constitucional (RE 418.416, Rel. Sepúlveda Pertence, Plenário, 10.5.2006)."
[711] Ressalvamos que, segundo expusemos no item 1.2, entendemos se tratar de um direito geral à intimidade.
[712] BADARÓ, 2010, p. 485.

pela garantia da inviolabilidade das comunicações, mas pela garantia geral da intimidade e da vida privada (art. 5º, X, CF)[713].

Antes de se adotar uma ou outra corrente, há que se definir quais, entre os mais diversos dados que possam repousar em bancos de dados, sejam os administrados por empresas dedicadas a comunicações, sejam por entidades de qualquer outra natureza, podem ser classificados como dados de tráfego de comunicações, sendo certo que tal verificação passa, como se verá, pela identificação dos limites do âmbito de proteção do direito à inviolabilidade do sigilo das comunicações.

Para Juan López (2012), o direito ao sigilo das comunicações protege os interlocutores das ingerências de terceiros e compreende qualquer modalidade de comunicação, existente ou que venha a existir, que ostente as características de se desenvolver a distância e por meio de algum artifício técnico, amparando, também, dados outros além dos relativos ao conteúdo da comunicação[714]. Afinal, prossegue o autor, "por una parte, la exclusión del ámbito de cobertura del derecho al secreto de las comunicaciones de ciertos datos de tráfico es contraria al alcance formal del derecho", mas, "por otra, la ampliación temporal del ámbito de cobertura del secreto de las comunicaciones ocasiona más problemas de los que resuelve, no se corresponde con el objeto del derecho de las comunicaciones y no es precisa para proporcionar um nivel de protección apropriado a los datos vinculados a las comunicaciones electrónicas al margen de la comunicación en curso"[715].

Conclui López afirmando que, "desde el punto de vista temporal, no constituye intervención de comunicaciones la obtención de información vinculada al servicio de comunicaciones electrónicas anterior o posterior al proceso de comunicación"[716].

Para o autor espanhol, portanto, o que definirá se o acesso a dados sobre comunicações distintos de seu conteúdo humano são protegidos pelo direito ao sigilo das comunicações será a autonomia de sua obtenção relativamente à medida de interceptação da comunicação. Noutras palavras, para López, os dados obtidos através de requisição oficial dirigida a determinado provedor ou companhia telefônica que independa de sua contemporaneidade em

[713] BADARÓ, 2010, p. 484/485. O autor também afasta o regime das interceptações das medidas tecnológicas utilizadas nas modernas investigações para a localização de pessoas e coisas, a exemplo do GPS (global position system) e da identificação ERB (estação radiobase) das companhias de telefonia celular. Embora fuja ao objeto do presente trabalho, observa-se que a localização via ERB ou GPS, esteja ela ou não submetida ao regime do sigilo das comunicações, constituiria, no Brasil, meio de obtenção de prova atípico, sem qualquer regulamentação e, portanto, inadmissível.
[714] LÓPEZ, 2012, p. 115.
[715] Ibid., p. 117.
[716] Ibid., p 119.

relação a comunicações em andamento não estarão inseridos no âmbito de proteção do direito ao sigilo das comunicações.

Voltando olhos ao que se levantou no presente trabalho acerca de ordenamentos estrangeiros[717], tem-se que a legislação inglesa foi por demais genérica ao listar os dados de tráfego como aqueles capazes de identificar as pessoas envolvidas na comunicação, os aparelhos e a localização de onde partiu a comunicação e para o qual ela foi enviada[718].

A Diretiva 2002/58 da Comunidade Europeia definiu dados de tráfego como "quaisquer dados tratados para efeitos do envio de uma comunicação através de uma rede de comunicações electrónicas ou para efeitos da facturação da mesma" (art. 2º, b), dispondo que podem ser relativos ao encaminhamento, à duração, ao tempo ou ao volume de uma comunicação, ao protocolo utilizado, à localização do equipamento terminal do expedidor ou do destinatário, à rede de onde provém ou onde termina a comunicação, ao início, fim ou duração de uma ligação, bem como ao formato em que a comunicação é enviada pela rede (art. 15).

A lei espanhola, por sua vez, foi adequadamente detalhista, porém excessiva ao definir os dados de tráfego como aqueles capazes de identificar os interlocutores, sesu telefones, endereços, IPs, data, hora e duração da comunicação, data e hora da conexão e desconexão do usuário à internet, endereço vinculado a determinado IP, hora da conexão e desconexão do usuário ao servidor de e-mail e identificação dos aparelhos e equipamentos[719].

Dizemos que foi excessiva porque bem mais razoável se mostrou o método de classificação adotado pelo Tribunal Supremo da Espanha ao definir quais dados deveriam estar inseridos no âmbito de proteção do direito ao sigilo das comunicações. Afirmou a Corte que os elementos externos protegidos por tal direito seriam aqueles ligados a alguma comunicação concreta, enquanto que aqueles desconectados de uma comunicação concreta estariam protegidos, simplesmente, pelo direito geral à intimidade.

Pela lógica espanhola acima referida, com a qual concordamos, seriam exemplos de dados que fogem à esfera de proteção do direito à inviolabilidade do sigilo das comunicações: os dados cadastrais de assinantes, tais como seu endereço e telefone; os dados identificadores de aparelhos (a exemplo do código IMEI) e do usuário (a exemplo do IMSI[720]); o IP do

[717] No capítulo 3.
[718] Ver item 3.2.6.
[719] Ver item 3.3.3.
[720] Ver as definições de IMEI e IMSI no item 2.2.4.

assinante pesquisado (quando for fixo ou estático[721]), mas jamais do interlocutor que possa ter-se comunicado com o alvo, por razões abaixo expostas.

Já os dados indissociáveis de comunicações concretamente ocorridas serão fatalmente dados que devem ser preservados sob o manto da proteção ao sigilo das comunicações. Exemplos são o IP (dinâmico) utilizado em determinada comunicação, a duração, data e hora de determinada comunicação, a hora de conexão e desconexão ao servidor de e-mail e a hora da conexão e desconexão à internet, bem como sua duração.

Estes últimos, em nossa ótica, são os que se podem classificar como dados de tráfego de comunicações, que passamos a tratar de *dados de tráfego de comunicações em sentido estrito*.

Não nos filiamos, portanto, ao chamado critério temporal, adotado pelo *Tribunal Constitucional de España*, no sentido de que o regime do sigilo das comunicações só se prestaria a proteger comunicações no momento em que elas estejam ocorrendo, ficando qualquer dado posterior, decorrente de comunicações finalizadas ou consumadas, protegido pela norma geral protetora da intimidade (naquele país, art. 18.1 da Constituição)[722].

Quanto à hora da conexão e desconexão à internet, bem como sua duração, o espanhol Juan López (2012) observou que tal conexão não constitui uma comunicação no sentido de transferência de mensagens emanadas de um interlocutor, mas uma condição para que a comunicação venha a se iniciar[723]. Apesar de correta a colocação de López, entendemos que horários de conexão e desconexão são dados vinculados a uma comunicação concreta na medida em que o momento em que ocorre a conexão marca o início do intercâmbio de dados, que, embora não necessariamente de conteúdo humano, já constitui inegavelmente uma comunicação telemática. Além disso, no plano prático, o regime de proteção incidente sobre os dados que tenham sido transmitidos imediatamente após uma conexão, ainda que não veiculem um conteúdo humano (mas apenas protocolos de sistema), seria indissociável do tratamento a ser dispensado aos conteúdos humanos, uma vez que o momento a se eleger um ou outro regime seria, naturalmente, anterior à descoberta do tipo de informação que transitou.

---

[721] Isto porque o IP variável ou dinâmico, para ser revelado, precisará estar vinculado a uma comunicação concreta.

[722] Precedente analisado no item 3.3.1 (TCE, Sentencia 70/2002, de 3 de abril de 2002, Sala Primera, Recurso de amparo nº 3787-2001, Fecha 03/04/2002).

[723] LÓPEZ, 2012, p. 123.

Já os dados de localização dos interlocutores[724] constituirão dados de tráfego de comunicações em sentido estrito se forem obtidos em razão da realização de uma comunicação concreta. Dados reveladores, por exemplo, da localização de um usuário que esteja portando um aparelho móvel, seja por meio de GPS, seja de ERBs, e sem que tal se dê em razão de uma comunicação que esteja ocorrendo ou tenha ocorrido, não poderão ser classificados como dados de tráfego de comunicações.

De forma coerente com esta mesma linha, discorda-se dos precedentes jurisprudenciais norte-americanos que julgaram não haver *expectation of privacy* nos dados relativos a números discados por assinantes[725], pois, embora se trate de questão mais atinente à interceptação telefônica, fugindo do tema do presente trabalho, os números discados, comparáveis a endereços de e-mails destinatários de mensagens ou a IPs de interlocutores que travaram comunicações com alguma pessoa-alvo de monitoramento, são inegavelmente reveladores da existência de uma comunicação concreta ocorrida e de seus interlocutores, o que se insere, sem sombra de dúvidas, no direito ao sigilo das comunicações.

Afinal, retirar os dados relativos a comunicações concretamente ocorridas do âmbito normativo do direito ao sigilo das comunicações não sobreviveria ao teste do critério da especificidade[726], pois tais dados, ainda que desacompanhados de seu conteúdo humano, não podem ser classificados como circunstâncias meramente acidentais do exercício do direito, mas, ao contrário, são aspectos específicos dele.

Acrescente-se que, segundo a teoria externa, aqui adotada, o direito existe de forma ilimitada, enquanto que, de outro lado, existem as restrições, decorrentes dos demais direitos existentes e das normas protetivas dos interesses da comunidade[727]. E a definição do âmbito normativo advirá, justamente, do conteúdo e da extensão dessas restrições. Portanto – e agora tratando do caso do Brasil –, se a Constituição de 1988 estabeleceu a inviolabilidade do sigilo das comunicações, o conteúdo e a extensão de eventuais restrições a ele precisarão advir de uma interpretação sistemática de outras normas constitucionais protetoras do interesse

[724] O art. 2º, b e c da Diretiva 2002/58/CE define os chamados "dados de localização" como "quaisquer dados tratados numa rede de comunicações electrónicas que indiquem a posição geográfica do equipamento terminal de um utilizador de um serviço de comunicações electrónicas publicamente disponível". Dispõe o art. 14 que "os dados de localização podem incidir sobre a latitude, a longitude e a altitude do equipamento terminal do utilizador, sobre a direcção de deslocação, o nível de precisão da informação de localização, a identificação da célula de rede em que o equipamento terminal está localizado em determinado momento e sobre a hora de registo da informação de localização."
[725] Ver casos *United States v. Knotts* e *Smith v. Maryland* no iten 3.1.4.
[726] Ver item 4.1.2.
[727] Ver item 4.1.2.

público, normas estas que, é claro, existem na Constituição, a exemplo dos mandamentos constitucionais de criminalização e do direito à segurança[728].

Mas, considerando que a inviolabilidade do sigilo das comunicações foi instituída constitucionalmente através de uma regra com restrição legal mediata qualificada[729], não é possível restringi-la sem que o seja através de dispositivo legal expresso (na Lei 9.296/96) que, em relação aos dados de tráfego, inexiste[730]. Noutras palavras, a Lei 9.296/96, prescrita pelo constituinte, pode listar hipóteses de afastamento da inviolabilidade do sigilo das comunicações, desde que o faça para fins de investigação criminal ou instrução processual penal, mas, se a referida lei não previu a possibilidade de violação dos dados externos às comunicações, há que se concluir que eles estão inseridos no âmbito de proteção do inciso XII do artigo 5º da CF, somente podendo ser violados se preenchidos os demais pressupostos legais necessários a permitir a violação do conteúdo humano das comunicações, tendo em vista que estes últimos são destinatários de proteção maior, conforme se passa a demonstrar a seguir. Noutras palavras, embora se reconheça que o conteúdo humano das comunicações seja merecedor de proteção maior do que os dados de tráfego, na falta de previsão legal especificando as hipóteses de restrição do sigilo sobre estes últimos, entendemos que eles só poderão ser restringidos junto com o sigilo incidente sobre o conteúdo humano das comunicações a que eles se referem.

Quanto ao nível de proteção que se deve dar aos dados de tráfego relativamente aos dados de conteúdo humano – e agora no recém-definido sentido estrito da expressão dados de tráfego –, discorda-se do decidido no caso Escher e outros vs. Brasil[731], em que a Corte IDH, ao considerar que ambos dizem respeito ao sigilo das comunicações, destinou aos dados de tráfego o mesmo tratamento dispensado aos dados de conteúdo.

Mais adequado foi o entendimento adotado no precedente do *Tribunal Constitucional de España*, ao reconhecer que o acesso a dados reveladores do destino, hora e duração das comunicações, embora inseridos no direito ao sigilo das comunicações, devem ser protegidos em menor intensidade do que o conteúdo humano das comunicações, ou seja, do que o teor que um interlocutor efetivamente pretendeu enviar ao outro[732].

---

[728] Ver item 4.1.2.
[729] Ver item 4.1.2.
[730] Para Antonio Scarance Fernandes, o sigilo sobre dados poderá ser afastado mediante autorização judicial, desde que previsto em lei, o que, no caso do sigilo fiscal, está regulado no Código Tributário Nacional e, no bancário, pela Lei Complementar (LC) nº 105/2001 (FERNANDES, 2008a, p. 244/245).
[731] Ver item 1.3.
[732] Ver item 3.3.3.

Parece-nos igualmente adequada a distinção de tratamento que o legislador inglês dispensou aos dados de tráfego comparativamente aos conteúdos comunicativos, no sentido de ter tornado mais fácil o acesso àqueles do que a estes. O rol de hipóteses nas quais é permitido o acesso a dados de tráfego – bem maior do que o relativo a conteúdos humanos[733] – mostra que o nível de proteção dispensado a estes no sistema inglês é adequadamente maior do que o que é dispensado àqueles.

Apesar disso, não nos parece razoável a possibilidade vigente na Inglaterra de que qualquer servidor integrante dos quadros dos órgãos de persecução requisite dados de tráfego diretamente às empresas de comunicações[734] ou, menos ainda, com a carta branca dada ao Secretário de Estado para deferir o acesso a tais dados em hipóteses não previstas em lei[735].

Afinal, tais prerrogativas investigativas não sobrevivem a um exame de proporcionalidade, porquanto desatendem aos subprincípios da exigibilidade material, espacial e pessoal, e ferem o direito à privacidade na extensão que lhe atribuíram as cortes internacionais. Senão, vejamos que a possibilidade irrestrita e demasiado aberta de requisição de dados de tráfego por qualquer investigador está longe de constituir o meio mais comedido possível de limitação ao direito fundamental (exigibilidade material), bem como longe está de zelar para que os interesses sacrificados sejam somente os da pessoa-alvo da medida (exigibilidade pessoal). Por sua vez, a prerrogativa do Secretário de Estado inglês de autorizar o acesso a dados de tráfego das comunicações em hipóteses não previstas em lei fere o subprincípio da exigibilidade espacial[736], porquanto deixa de limitar o âmbito de intervenção, ferindo, também, a proteção à vida privada na extensão que lhe atribuíram as cortes internacionais, que exigem a expressa previsão legal[737].

Quanto à necessidade ou não de intervenção judicial para viabilizar o acesso aos dados de tráfego pelos órgãos de persecução, há no Brasil uma necessidade maior de reflexão para se chegar a uma resposta do que na situação da Inglaterra e da Espanha, pois, no primeiro país, a lei é clara quanto à dispensa de ordem judicial[738], enquanto, no segundo, a lei é clara no sentido oposto, ou seja, da exigência de autorização judicial para o acesso a dados de tráfego de comunicações[739].

---

[733] Ver item 3.2.6.
[734] Ver item 3.2.6.
[735] Ver item 3.2.6.
[736] Sobre os subprincípios do prinípio da proporcionalidade, ver item 1.4.
[737] Ver item 1.3.
[738] Aliás, nem para interceptar o conteúdo humano das comunicações na Inglaterra necessita-se de ordem judicial. Ver item 3.2.3.
[739] Ver item 3.3.3.

Já no Brasil, onde, tal qual nos Estados Unidos[740], não há dispositivo legal expresso neste sentido, é preciso examinar se haverá necessidade de ordem judicial com base em fontes diversas.

Quanto ao que já se definiu acima sob a designação de dados de tráfego de comunicações em sentido estrito, ou seja, aqueles vinculados a comunicações concretas, a conclusão no sentido de que se encontram dentro do âmbito normativo do direito à inviolabilidade do sigilo das comunicações não deixa dúvida de que o acesso a este dependerá de ordem judicial prévia, posto que é o próprio dispositivo constitucional quem o exige (art. 5º, XII, CF).

No entanto, uma vez deferida a interceptação do conteúdo humano das comunicações telemáticas de determinado indivíduo, deve-se dispensar a necessidade de ordem judicial especificamente voltada para deferir também o acesso aos dados de tráfego daquelas mesmas comunicações pertencentes àquele mesmo indivíduo. Isto porque, além de o acesso a esses dados ser inegavelmente menos gravoso do que a interceptação de conteúdo, para se assegurar a necessária eficiência da interceptação, revela-se imprescindível que o agente investigador conte, durante a execução da medida, com a possibilidade de verificar, e com agilidade, todos os dados relativos às comunicações de seu alvo, até para verificar a necessidade de ampliação da medida sobre outros indivíduos que se comuniquem com o alvo, bem como de levantar, enfim, todos os dados possíveis sobre ele. Ademais, os dados externos a comunicações concretamente realizadas lhes são acessórios.

Dito isto sobre a necessidade de ordem judicial para acesso aos dados de tráfego de comunicações em sentido estrito, resta verificar como se deve fazer em relação a todos os demais dados relativos a comunicações, que não o próprio conteúdo humano ou os dados de tráfego em sentido estrito. Para tanto, há que se examinar se estes estarão inseridos na proteção geral à intimidade (art. 5º, X).

Para executar tal exame, mostra-se aplicável o critério tão recorrente nos acórdãos norte-americanos, no sentido de se identificar a presença ou ausência de *expectation of privacy*. Apesar das diferenças conhecidas entre aquele ordenamento e o brasileiro, não se vislumbra qualquer impedimento à "importação" do raciocínio, segundo o qual dependerá de ordem judicial o acesso a todo e qualquer dado sobre o qual o indivíduo deposite alguma *expectation of privacy*, desde que seja legítima e que a sociedade esteja preparada para reconhecer a expectativa como razoável[741].

---

[740] Ver item 3.1.4.
[741] Ver item 3.1.1.

Isto porque, antes de o Estado ter condições de frustrar a *expectation of privacy* do indivíduo, será preciso um exame de proporcionalidade, que não se imagina sendo feito por outro servidor público que não uma autoridade judiciária[742]. Afinal, o zelo pelo equilíbrio entre meios e fins, pela menor ingerência possível sobre os direitos individuais e pela aptidão do meio para obter o fim pretendido para realizar o interesse público, devendo haver prova desta aptidão, precisa ser realizado por autoridade dotada de garantias funcionais que permitam sua imparcialidade, sob pena de violação, ademais, ao núcleo essencial de garantias[743].

E não se tem dúvida em afirmar que, não só os dados vinculados a comunicações ocorridas concretamente são destinatários de expectativa de privacidade, mas também aqueles não vinculados a comunicações concretas podem sê-lo.

Veja-se que, quando um indivíduo preenche dados cadastrais[744] num provedor de internet, ele não espera, evidentemente, que tais informações estejam ao acesso de qualquer um, verificando-se sobre eles, portanto, inegável expectativa de privacidade, razão pela qual o acesso a estes deve também ser precedido de ordem judicial.

Mas, se tanto o acesso do Estado aos dados preservados sob a proteção geral à intimidade, quanto àqueles protegidos pelo sigilo das comunicações dependerão de ordem judicial, qual será a relevância prática de tantas classificações e reflexões?

É que, no caso dos dados protegidos sob o direito ao sigilo das comunicações, seja conteúdo, sejam os dados de tráfego de comunicações em sentido estrito, o magistrado estará obrigado a seguir o regime da Lei 9.296/96, enquanto que, diante das informações protegidas pelo direito geral à intimidade, deverá o juiz seguir regime diverso, qual seja, o da busca e apreensão, previsto nos artigos 240 e seguintes do CPP.

Observe-se, no entanto, que o Projeto de Código de Processo Penal estabelece que o acesso estatal "aos registros de dados estáticos referentes à origem, destino, data e duração das ligações telefônicas, igualmente protegidos por sigilo constitucional" (art. 246, §2º) seguirá seção própria, intitulada "Do acesso a informações sigilosas" (art. 241 e seguintes), que é distinta daquela destinada a regular a busca e apreensão (art. 228 e seguintes). Enquanto a última impõe apenas a existência de "indícios suficientes de que alguém oculta os objetos que possam servir de prova de infração penal", a primeira exige "indícios razoáveis da prática

[742] Sobre a reserva de jurisdição exigida para se impor restrição ao direito à inviolabilidade do sigilo das comunicações, ver item 4.5.
[743] Sobre o conceito de núcleo essencial de garantias, ver item 1.4.
[744] López se refere aos dados cadastrais como "Datos de suscripción o datos de abonado", definindo-os como "aquellos que constituyen la información personal recabada del abonado a la hora de subscribir el contrato de prestación de servicios de comunicación" (LÓPEZ, 2012, p. 121).

de infração penal que admita a providência", "a necessidade da medida, diante da impossibilidade de obtenção da prova por outros meios" e, por fim, "a pertinência e a relevância das informações pretendidas para o esclarecimento dos fatos"[745].

Entendemos que o tratamento dados aos dados de tráfego pelo Projeto se mostra eficiente, porque, além de permitir uma adequada persecução penal, possibilita a incidência real das normas de garantia. É, neste ponto, ademais, consentâneo com o princípio da proporcionalidade, porquanto restringe aos casos envolvendo crimes de um catálogo[746] (exigibilidade espacial) a possibilidade de acesso aos dados de tráfego, exige a pertinência e a relevância das informações pretendidas para o esclarecimento dos fatos (proporcionalidade em sentido estrito), bem como a demonstração da necessidade da medida diante da impossibilidade de obtenção da prova por outros meios (exigibilidade espacial).

4.12 Interceptação preventiva

Ao comentar o filme futurista *Minority Report*, Danilo Dias Ticami e Poliana Soares Albuquerque (2012) observaram que, possivelmente, uma das maiores frustrações do direito penal, especialmente em tempos de busca pela eficiência, seja o fato de ser um instrumento que sempre chegará atrasado, após o bem jurídico tutelado pela norma ser colocado em risco, revelando-se o direito penal, por isso, "um instrumento desajeitado e com limitada (e discutível) atuação, especialmente por força do princípio da lesividade e pela proibição de punição dos atos preparatórios"[747].

Mas, enquanto nos Estados Unidos, a *Section* 2518 do *Title* 18 do USC contempla a possibilidade de interceptação de comunicações tendo por objeto um crime de seu catálogo que esteja "*about to be committed*", ou seja, prestes a ser cometido[748], e, na Inglaterra, a *Section* 5(3)b do RIPA 2000 permite interceptação "*for the purpose of preventing or detecting*

[745] Parecer nº 1.636, de 2010, estabelecendo a redação final do Projeto de Lei do Senado nº 156, de 2009. Em: http://www.senado.gov.br/atividade/materia/getPDF.asp?t=85509&tp=1

[746] O catálogo, se é que assim se pode classificá-lo, é composto de todos os tipos penais, exceto as contravenções e crimes de menor potencial ofensivo (Projeto, art. 247).

[747] TICAMI, Danilo Dias; ALBUQUERQUE, Poliana Soares. Minority Report: a nova lei e velhos devaneios repressivistas. In: **Revista Liberdades** - nº 11 - setembro/dezembro de 2012, Publicação Oficial do Instituto Brasileiro de Ciências Criminais.

[748] Ver item 3.1.5.

serious crime"[749-750], que, em tradução livre, significa para prevenir ou detectar crime grave, no Brasil a realidade é distinta.

Isto porque, apesar de uma espécie de carta branca que o constituinte brasileiro deu ao Estado em relação às interceptações telefônicas na hipótese de Estado de Defesa (e não o fez quanto às telemáticas), as únicas exceções constitucionais à inviolabilidade do sigilo das comunicações se dão para fins de "investigação criminal" e "instrução processual penal", o que no "sentido usual da técnica legislativa pátria" só podem ocorrer em relação a crimes pretéritos[751].

O Projeto de Código de Processo Penal, no entanto, trouxe a previsão de interceptação "quando a vida de uma pessoa estiver em risco" (art. 250, §1º), mas, caso aprovado, a interpretação constitucional do dispositivo, bem como a sistemática em relação ao restante do arcabouço normativo brasileiro continuarão a exigir um crime pretérito, para que haja, senão um processo, ao menos uma investigação criminal, no sentido legal da expressão.

Mas, mesmo ciente da impossibilidade de se conceber interpretações frontalmente contrárias ao texto constitucional, tal qual se posicionou Canotilho (2000) em relação ao chamado método jurídico de hermenêutica[752], não vislumbramos uma vedação constitucional expressa à existência de uma interceptação preventiva. É que a exigência de que tenha ocorrido um crime, no sentido usual da palavra, portanto pretérito, é o fato de não haver previsão legal de investigação criminal voltada para impedir crimes futuros, de modo que o que separa a realidade atual de uma realidade em que haja investigação sobre crimes ainda não cometidos é, tão somente, a disciplina infraconstitucional de tal modalidade investigativa.

Hoje, portanto, o cenário legislativo brasileiro torna ilegal uma interceptação preventiva, não em razão de veto constitucional, mas em respeito à ausência de concepção legal de uma investigação criminal relativa a crime futuro. Enquanto pendente uma adequação legislativa que seja capaz de prever uma investigação relativa a crime futuro, o ato de promover interceptação preventiva afrontaria a exigência, recorrente nas cortes internacionais, de previsão legal da medida[753], além do que esta constituiria prova atípica segundo qualquer das duas concepções, a ampliativa ou a restritiva[754].

---

[749] Na Inglaterra, também a requisição de dados de tráfego pode ser feita, segundo a *Section* 22(2)2 do RIPA 2000, "for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health" (Ver item 3.2.6).
[750] Ver item 3.2.3.
[751] BADARÓ, 2010, p. 497.
[752] Ver item 4.1.3.
[753] Ver item 1.3.
[754] Ver item 4.2.

Isto, no entanto, não afastaria, por óbvio, que, em situações-limite, para salvar vidas ou proteger outro bem jurídico de altíssima relevância, incidisse causa excludente de ilicitude em caso de interceptação não autorizada.

4.13 As tecnologias de criptografia e sua regulamentação

O Brasil não conta com nenhuma regulamentação legal sobre o uso de tecnologia voltada para criptografar as comunicações, método empregado para torná-las mais seguras.

O Projeto de Lei 5.285, de 2009, da Câmara dos Deputados, no parágrafo único de seu artigo 21, busca criminalizar, com pena de dois a oito anos, aquele que "utiliza a criptografia para proteger comunicação de voz, imagem e dados, em desacordo com as normas expedidas pelo órgão federal competente"[755].

O "órgão federal competente", por sua vez, será, segundo o artigo 28 do mesmo Projeto, a Agência Nacional de Telecomunicações (ANATEL), a quem cumprirá disciplinar "o padrão tecnológico, os procedimentos relativos à produção, comercialização, importação e o uso da criptografia e de sistemas de interceptação" (art. 28, §1º). O Projeto também obriga o fabricante de tecnologia de criptografia a depositar previamente na ANATEL a chave de acesso capaz de decodificá-la (art. 28, §2º)[756].

---

[755] Art. 21. Constitui crime produzir, fabricar, importar, comercializar, oferecer, emprestar, adquirir, possuir, manter sob sua guarda ou ter em depósito,sem autorização ou em desacordo com determinação legal ou regulamentar, equipamentos destinados especificamente à interceptação, escuta, gravação e decodificação das comunicações telefônicas, incluindo programas de informática e aparelhos de varredura: Pena - reclusão, de dois a oito anos, e multa. Parágrafo único. Incorre na mesma pena quem utiliza a criptografia para proteger comunicação de voz, imagem e dados, em desacordo com as normas expedidas pelo órgão federal competente (BRASIL. Câmara dos Deputados. PL 5.285/2009, apresentado em 27.05.2009, pela Comissão Parlamentar de Inquérito instaurada com a finalidade de investigar escutas telefônicas clandestinas/ilegais, conforme denúncia publicada na Revista "Veja", edição 2022, nº 33, de 22 de agosto de 2007. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=436096>. Acesso em: 05 jan. 2014).

[756] Art. 28. A ANATEL – Agência Nacional de Telecomunicações fiscalizará as prestadoras de serviços de telecomunicações exigindo delas o cumprimento das normas técnicas determinadas pelos órgãos competentes. §1º A Agência de que trata o *caput*, ouvido o Instituto Nacional de Tecnologia da Informação – ITI, disciplinará o padrão tecnológico, os procedimentos relativos à produção, comercialização, importação e o uso da criptografia e de sistemas de interceptação. §2º A chave de acesso de qualquer comunicação criptografada deverá ser previamente depositada na ANATEL, nos termos do regulamento de que trata o parágrafo anterior (BRASIL. Câmara dos Deputados. PL 5.285/2009, apresentado em 27.05.2009, pela Comissão Parlamentar de Inquérito instaurada com a finalidade de investigar escutas telefônicas clandestinas/ilegais, conforme denúncia publicada na Revista "Veja", edição 2022, nº 33, de 22 de agosto de 2007. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=436096>. Acesso em: 05 jan. 2014).

A exigência pretendida pelo Projeto se assemelha em muito à influência exercida pela NSA sobre o NIST (*National Institute of Standards and Technology*), nos Estados Unidos, no sentido de influenciar os padrões utilizados pelos sistemas de criptografia.

Na Inglaterra, conforme abordado no item 3.2.8, se o material interceptado estiver ilegível em razão de criptografia, qualquer investigador na condução legal de uma investigação que necessitar do código para decifrá-la poderá representar a um juiz pugnando por uma *appropriate permission*, autorização que lhe concede o poder de expedir uma determinação dirigida a quem possui a chave ou senha para que a forneça em prazo determinado, sob pena de incorrer em crime com pena de até cinco anos de reclusão.

Impossível não notar a ligação entre a criminalização da recusa em fornecer chave para abrir uma criptografia e o direito de não se autoincriminar. No precedente inglês *R v S and another*, os acusados alegaram, perante a *Criminal Division* da *Court of Appeal* da Inglaterra, que sua recusa em fornecer a chave de acesso a material protegido por criptografia foi a base da acusação formulada contra eles, o que seria incompatível com o privilégio contra a autoincriminação, além de afrontar a garantia de processo equitativo assegurada no artigo 6º da Convenção Europeia.

Entendeu a Corte, no entanto, que a incursão no privilégio contra a autoincriminação no caso foi legítima e proporcional, já que o material protegido por criptografia tinha sua existência independente das mentes dos acusados, tal qual ocorreria com impressões digitais, amostras de sangue e gravações de voz, e que a chave de acesso em si, que estava na mente dos acusados, não constituiria elemento criminoso por si só[757].

Já na Espanha, a *Ley General de Telecomunicaciones* autoriza expressamente o uso de criptografia, que o diploma define como um instrumento de segurança da informação, mas estabelece, entre suas condições de uso, a prerrogativa do Estado de impor a obrigação de facilitar a um órgão estatal, sem custo algum, os meios e equipamentos para descriptografar a comunicação[758].

Entendemos que a criminalização do uso de criptografia protetora do sigilo das comunicações, acaso adotada no Brasil, iria na contramão do próprio texto constitucional, na medida em que a criptografia serve justamente a proteger bens jurídicos já protegidos pela própria Constituição: a inviolabilidade do sigilo das comunicações, da intimidade e da privacidade.

---

[757] Ver item 3.2.8.
[758] Ver item 3.3.4.

Criminalizar seu uso ou exigir que os meios de violação da criptografia sejam previamente entregues à ANATEL seria como exigir que cada cidadão deixasse a porta de sua residência destrancada ou que fornecesse uma cópia da chave ao Estado, de modo a facilitar-lhe o ingresso.

Assim como a porta trancada não tem a finalidade única de dificultar o ingresso das forças do Estado, servindo também para afugentar a ação de invasores de toda sorte, a criptografia também se presta a proteger segredos das mais diversas espécies, atinentes desde os assuntos relativos à vida privada de cada um até os segredos industriais, financeiros e até de Estado.

Sintomáticas, nesse sentido, foram duas manifestações do Senado Federal relativas ao tema, a primeira em 2004 e a segunda em 2013.

Em 2004, o Senado, com fulcro no artigo 50, §2º da CF[759], pediu explicações ao Ministro-Chefe do Gabinete de Segurança Institucional da Presidência da República sobre a notícia jornalística de que o governo teria encomendado à ABIN a produção de telefones celulares privilegiados e protegidos por criptografia para uso de Ministros de Estado e outros servidores diretos da Presidência. Solicitou o Senado, então, que a Presidência "especifi[casse] o significado desse projeto, custos e destinação exata, bem como que se indi[casse] a motivação para esse privilégio"[760].

Anos depois, em 2013, após o escândalo Snowden, a Comissão de Relações Exteriores e Defesa Nacional do Senado propôs a realização de audiência pública "com o objetivo de tratar das vulnerabilidades do Estado brasileiro no setor cibernético, constatadas recentemente com a denúncia de espionagem norte-americana. Agências governamentais dos EUA estariam fazendo acompanhamento, em larga escala, de *e-mails* e ligações telefônicas a nível internacional, de cidadãos e empresas, inclusive no Brasil"[761].

---

[759] Constituição Federal. Art. 50. A Câmara dos Deputados e o Senado Federal, ou qualquer de suas Comissões, poderão convocar Ministro de Estado ou quaisquer titulares de órgãos diretamente subordinados à Presidência da República para prestarem, pessoalmente, informações sobre assunto previamente determinado, importando crime de responsabilidade a ausência sem justificação adequada.(Redação dada pela Emenda Constitucional de Revisão nº 2, de 1994) § 1º - Os Ministros de Estado poderão comparecer ao Senado Federal, à Câmara dos Deputados, ou a qualquer de suas Comissões, por sua iniciativa e mediante entendimentos com a Mesa respectiva, para expor assunto de relevância de seu Ministério. § 2º - As Mesas da Câmara dos Deputados e do Senado Federal poderão encaminhar pedidos escritos de informações a Ministros de Estado ou a qualquer das pessoas referidas no caput deste artigo, importando em crime de responsabilidade a recusa, ou o não - atendimento, no prazo de trinta dias, bem como a prestação de informações falsas. (Redação dada pela Emenda Constitucional de Revisão nº 2, de 1994)

[760] BRASIL. Senado Federal. SF RQS 1224/2004 de 14.09.2004. Autor: Senador Arthur Virgílio. Disponível em: <http://www.senado.gov.br/atividade/materia/detalhes.asp?p_cod_mate=70061>. Acesso em: 06 jan. 2014.

[761] BRASIL. Senado Federal. SF RRE 68/2013 de 08.08.2013. Autor: Senador Ricardo Ferraço. Disponível em: <http://www.senado.gov.br/atividade/materia/detalhes.asp?p_cod_mate=113884>. Acesso em: 06 jan. 2014.

Portanto, da pior maneira, mostrou-se ao Senado que algo antes visto como privilégio constitui, no mundo moderno, artigo de primeira necessidade.

Os episódios demonstram que não só para fins criminosos os cidadãos, e as autoridades, se servem de equipamentos que dificultam a violação do sigilo de suas comunicações.

A nosso ver, o direito do cidadão de usar meios adicionais para proteger o sigilo de suas próprias comunicações, como a criptografia, está compreendido no âmbito de proteção do direito ao sigilo das comunicações.

Afinal, pelo critério da especificidade (Müller)[762], temos que o uso de criptografia se mostra um ato específico do exercício do direito à inviolabilidade do sigilo das comunicações, e não uma circunstância meramente acidental (Mendes; Coelho; Branco)[763] de seu exercício.

Mais do que uma ação estruturalmente necessária (Virgílio Afonso da Silva)[764] ao exercício do direito ao sigilo das comunicações, entendemos que aquele que instala um sistema de criptografia para proteger suas comunicações está praticando um ato *inerente* ao próprio direito fundamental.

A regra da inviolabilidade do sigilo das comunicações estabeleceu esse direito com uma *reserva de lei restritiva* (Canotilho) ou com uma *restrição indiretamente constitucional* (Alexy)[765], delegada à Lei 9.296/96, sendo certo que ela, como qualquer outro diploma infraconstitucional que se pretenda restritivo de um direito fundamental, precisa ser uma norma compatível com a Constituição[766], sob pena de que a pretendida restrição se transfigure em violação e de que se acabe por esvaziar o direito em questão.

E o instrumento a se recorrer para avaliar a aceitabilidade dos níveis de restrição que uma norma gera a um direito fundamental vem a ser o princípio da proporcionalidade, com base no qual concluímos que a proibição generalizada e irrestrita do uso de criptografia atenderia o subprincípio da adequação, porquanto é apta a obter, mais comodamente, o fim pretendido pelo interesse público persecutório, mas não atenderia os dois outros subprincípios do princípio da proporcionalidade, quais sejam, o da exigibilidade e o da proporcionalidade em sentido estrito.

O da exigibilidade restaria desatendido porque o Estado estaria lançando mão de um meio nada comedido (exigibilidade material), sem a mínima limitação em seu âmbito de

[762] Ver item 4.1.2.
[763] Ver item 4.1.2.
[764] Ver item 4.1.2.
[765] Ver item 4.1.2.
[766] ALEXY, 2011, p. 281.

intervenção (exigibilidade espacial) e sem que os sacrifícios impostos se restringissem somente à pessoa do imputado (exigibilidade pessoal). A proporcionalidade em sentido estrito, por sua vez, restaria desatendida porquanto não haveria equilíbrio entre as vantagens do fim (facilitação na interceptação das comunicações daquela pequena parcela da população que o Estado necessite monitorar) e as desvantagens do meio, no caso incidentes sobre tudo e todos, de modo a fragilizar o direito ao sigilo das comunicações de um número indeterminado de pessoas[767].

[767] Faz lembrar a análise Christopher Soghoian (ver item 2.2.1) sobre a inserção irrestrita de vulnerabilidades intencionais (*backdoors*) em sistemas de comunicação, o que gera a exposição de todos os usuários, e não apenas os alvos das agências de inteligência, pois a providência aumenta significativamente a dificuldade de se desenvolver um produto seguro.

CONCLUSÃO

As conclusões a que chegamos sobre cada aspecto da pesquisa foram expostas ao longo do trabalho, notadamente no capítulo 4, no qual analisamos a interceptação das comunicações telemáticas no Brasil e as comparamos, onde coube, com as experiências dos países abordados no capítulo 3.

Passamos, então, a pontuar essas conclusões:

1) A norma inscrita no artigo 5º, inciso X, da CF, atinente à inviolabilidade da intimidade e da vida privada, é um princípio, do qual já emana um direito à inviolabilidade do sigilo das comunicações, ainda que este último não contasse com a previsão constitucional autônoma. Já a norma do artigo 5º, inciso XII, da CF se apresenta como uma regra constitucional, que permite ao indivíduo excluir do conhecimento de terceiros indesejados, aí incluído, é claro, o próprio Estado, o conteúdo de suas comunicações;

2) Na leitura desses direitos sob análise, adotamos a teoria externa, pela qual existem, de um lado, os direitos fundamentais e, de outro, as restrições, que decorrem dos demais direitos fundamentais e das normas protetivas de interesses da comunidade. O direito à inviolabilidade da intimidade e da vida privada (art. 5º, X da CF), portanto, concebido sem qualquer restrição, é voltado para proteger o indivíduo na maior extensão possível, de modo que, se o indivíduo não invadisse a esfera de proteção de outro indivíduo ou outros interesses sociais, sua proteção deveria ser, hipoteticamente, assegurada de modo absoluto. O mesmo deverá ocorrer com o direito à inviolabilidade do sigilo das comunicações (art. 5º, XII da CF), que, salvo se houver preenchimento da cláusula de exceção inserida na parte final do dispositivo, deve ser visto como um direito sem restrições;

3) Mas o constituinte brasileiro de 1988 concebeu o direito ao sigilo das comunicações nele fazendo inserir uma cláusula de exceção, por meio da qual delegou ao legislador ordinário, através do método chamado de restrição legal qualificada, o estabelecimento das hipóteses e das formas pelas quais se poderiam impor restrições ao direito, desde que o faça para fins de investigação criminal ou instrução processual penal. Tal delegação foi cumprida pelo legislador infraconstitucional por meio da Lei 9.296/96;

4) Ante as possíveis interpretações do artigo 5º, XII, temos que o texto constitucional não impôs ao sigilo das comunicações de dados e telefônica uma inviolabilidade absoluta;

5) A medida de interceptação das comunicações telemáticas é uma providência cautelar que constitui um meio de obtenção de prova típico, sendo seu resultado uma fonte de prova e o material por ela coletado, que, via de regra, estará contido numa mídia digital, um meio de prova documental, a ser inserido no processo;

6) Já se a medida for implementada durante a instrução processual, seu resultado ganharia a classificação, não de fonte de prova, mas de ato de prova, mas fizemos ressalva quanto a seu cabimento em tal fase. É que, para viabilizar a real participação das partes na relação jurídica processual, o contraditório há que ser pleno e efetivo, o que evidencia a relação entre o contraditório e o princípio da igualdade, que será instrumento de eliminação de qualquer desigualdade, jurídica ou de fato, entre os sujeitos do processo. Na fase judicial, quando o ex-investigado já ostentará a condição de sujeito processual, acusação e defesa se encontrarão em pleno exercício da dialética baseada em contraditório pleno, não se podendo permitir que se lance mão de medida, como a interceptação das comunicações do réu, capaz de romper a igualdade. No curso da instrução, ademais, o réu, não raro, travará constantes diálogos sobre suas estratégias defensivas, e não necessariamente só com seu defensor. Em tal momento, portanto, eventual implementação de interceptação das comunicações do réu violaria o princípio da paridade, pelo que concluímos que a interpretação mais equilibrada da expressão constitucional "instrução processual penal" (art. 5º, XII, CF) é a de que o produto da diligência de interceptação de comunicações poderá sim ser utilizado para fins probatórios na fase processual, porém a medida somente poderá ser implementada, executada na fase preliminar;

7) Numa classificação em que as comunicações travadas em *canal abierto* estão fora do âmbito de proteção do direito ao sigilo das comunicações (porquanto realizadas sem nenhuma expectativa de privacidade) e aquelas travadas em *canal cerrado* estão dentro dele, temos que a comunicação estabelecida pelo indivíduo com 20 ou mais interlocutores, embora em vias comunicativas fechadas (a exemplo de correntes de e-mail, *sites* de relacionamento e *chats*), importa em declínio tácito do direito ao sigilo, fazendo excluir aquela comunicação do âmbito de proteção do direito;

8) Os dados externos ao processo comunicativo ou dados de tráfego que se inserem no âmbito de proteção do direito ao sigilo das comunicações são aqueles vinculados a

comunicações concretamente realizadas, que classificamos como dados de tráfego de comunicações em sentido estrito. Exemplos deles são os registros de data e horário de e-mails transmitidos, os dados de um interlocutor que se comunicou com o alvo, a duração de comunicação que efetivamente aconteceu, o IP dinâmico utilizado numa determinada comunicação;

9) Retirar tais dados do âmbito normativo do direito ao sigilo das comunicações não sobreviveria ao teste do critério da especificidade[768], pois, ainda que desacompanhados do conteúdo humano das comunicações a que eles se referem, não há como classificá-los como circunstâncias meramente acidentais do exercício do direito;

10) Fora da esfera de proteção do direito à inviolabilidade do sigilo das comunicações estão os dados cadastrais de assinantes, tais como seu endereço e telefone, os dados identificadores de aparelhos (IMEI) e de usuários (IMSI) e o IP (fixo) do assinante pesquisado;

11) Embora os dados de tráfego devam ser protegidos em menor intensidade do que o conteúdo humano das comunicações, se a Lei 9.296/96 não previu a possibilidade de violação de dados de tráfego, colhe-se, como resultado, que estes somente poderão ser violados junto com os dados de conteúdo das comunicações a que eles se referem, desde que preenchidos os pressupostos legais necessários à interceptação desse conteúdo;

12) Os dados de tráfego são elementos acessórios ao conteúdo das comunicações a que eles se referem. Por isso, uma vez já deferida a interceptação do conteúdo humano das comunicações telemáticas de determinado indivíduo, dispensa-se a necessidade de ordem judicial especificamente voltada para deferir também o acesso aos dados de tráfego daquelas mesmas comunicações;

13) Quanto aos dados de tráfego não vinculados a comunicações concretas, e, portanto, fora do âmbito de proteção do direito ao sigilo das comunicações, o acesso a estes dependerá também de ordem judicial desde que o indivíduo neles deposite legítima expectativa de privacidade, sendo certo, no entanto, que a possibilidade de acesso do Estado a eles seguirá o regime de proteção geral à intimidade (art. 5º, X, CF), devendo o exame do magistrado decidir com base nos artigos 240 e seguintes do CPP;

14) Definidos os dados de tráfego de comunicações que estão e os que não estão no âmbito de proteção do direito ao sigilo das comunicações, temos que os primeiros se sujeitam

[768] Ver item 4.1.2.

ao mesmo regime das interceptações, dependendo o seu acesso pelo Estado de ordem judicial, no moldes da Lei 9.296/96;

15) O mesmo acontece em relação a processos comunicantes cujos dados de conteúdo humano deles decorrentes se perenizem, como ocorre com o e-mail, que está inserido no âmbito de proteção do direito ao sigilo das comunicações. A comunicação via e-mail, portanto, não se sujeita à inviolabilidade absoluta;

16) Pela mesma lógica, caso dados de tráfego em sentido estrito ou dados de conteúdo humano de comunicações venham a ser fisicamente apreendidos no *hard disk* de um investigado, o acesso estatal a eles dependerá de autorização judicial específica, submetida às mesmas exigências da Lei 9.296/96;

17) A interpretação do termo "necessária", constante do artigo 4º da Lei 9.296/96, deve ser sistemática e restritiva, de modo a evitar a chamada generosidade nas autorizações judiciais de interceptação. A exigência de que a medida de interceptação seja necessária constitui positivação do princípio da proporcionalidade, precisamente em seu subprincípio denominado necessidade ou menor ingerência possível, que orienta o intérprete a optar pela intervenção mínima, pela alternativa menos gravosa, obrigando-o a fazer uma comparação da interceptação com outras medidas aptas a satisfazer o fim perseguido e, ao final, levá-lo a eleger aquela menos lesiva para os direitos individuais;

18) O legislador norte-americano se aproximou dos padrões de eficiência e garantismo mais do que o brasileiro ao inserir dispositivo determinando que, tanto no requerimento de autorização para interceptação, quanto na decisão que a concede, deverá constar a descrição de procedimentos investigatórios normais que tenham sido tentados e falharam ou a exposição das razões pelas quais tais procedimentos não foram tentados, já que, por sua natureza, seriam incapazes de atingir o objetivo probatório pretendido ou que seriam perigosos demais;

19) O Estado não poderá lançar mão da interceptação de comunicações como primeiro ato investigatório;

20) Quanto aos crimes que admitem interceptação telemática no Brasil, a proposta doutrinária de deixar a questão totalmente a critério do juiz, sem a previsão legal de um catálogo, implicaria em ampliar de forma desmedida a margem de discricionariedade do juiz, o que iria contra, inclusive, a interpretação que o TEDH deu ao artigo 8º da CEDH. Ademais, ainda que a lei brasileira tivesse previsto, tal qual se fez na Inglaterra, que a

autoridade a conceder autorização estivesse obrigada a decidir com base no princípio da proporcionalidade, a ausência de um rol de crimes previsto em lei importaria em ferimento ao subprincípio da exigibilidade espacial, que, dirigido principalmente ao legislador, exige limitações ao âmbito da intervenção que o Estado promoverá sobre os direitos do indivíduo;

21) Ao admitir a interceptação para todo e qualquer crime punido com pena de reclusão, inadmitindo-a para todos os outros, não andou bem o legislador brasileiro, que deveria ter estabelecido um rol de crimes baseando-se, não só no critério da gravidade abstrata do crime, mas também no *modus operandi* de seu cometimento, de forma que, além dos crimes graves – e aqui haver-se-ia que incluir todos aqueles que sejam objeto de mandamento constitucional de criminalização –, deveriam ser passíveis de interceptação todos aqueles crimes ou contravenções que, embora de menor potencial ofensivo, fossem praticados através de meios de comunicação, como telefone, e-mail, *Facebook* ou outro veículo de baseado em internet ou comunicação digital. No entanto, a legislação brasileira atual, ainda que merecedora das críticas acima nesse ponto, afastou-se menos dos parâmetros de eficiência e garantismo do que a dos Estados Unidos, que admitiu a medida para todo e qualquer crime federal;

22) Quanto ao prazo de duração da interceptação, a legislação brasileira não cuidou de dar às partes meios de fiscalizar, ainda que *a posteriori*, a obediência aos períodos autorizados numa interceptação realizada na fase investigatória. Isto porque não há registro obrigatório nos autos do início efetivo da captação, tendo o réu que se basear apenas nas datas das decisões que autorizaram o início e as prorrogações da medida e nos ofícios remetidos às empresas de comunicação. Foi bem elaborada, neste sentido, a redação do Projeto de CPP, na medida em que, ao impor à empresa de telefonia o dever de comunicar diretamente ao juiz a data de início do desvio das comunicações para o órgão investigativo, faz registrar nos autos o momento exato do início da interceptação, permitindo aos sujeitos processuais, especialmente ao réu, um exercício mais efetivo de seu direito de defesa, que, neste ponto, dependerá da aferição, ainda que *post facto*, da regularidade da interceptação. Não tão eficiente, mas melhor do que a legislação brasileira atual neste ponto é a dos Estados Unidos, que, embora fixe marcos temporais para o início da medida, o faz com base em presunções (considera-se o início a manhã do dia em que a interceptação começa a ser executada ou, senão, o décimo dia depois que a autorização for expedida);

23) Quanto ao prazo de duração da interceptação propriamente dito, o princípio da proporcionalidade, em seu subprincípio denominado exigibilidade temporal, exige rigorosa delimitação no tempo de medida restritiva de direito fundamental, devendo essa delimitação estar disciplinada em lei. A lei brasileira, que, de fato, até poderia conter redação mais precisa quanto à impossibilidade de sucessivas renovações (art. 5º, Lei 9.296/96), há que receber interpretação restritiva em favor do direito individual ao sigilo das comunicações, não se podendo permitir que as interceptações perdurem além do prazo nela estabelecido, a saber, o de quinze dias prorrogável por igual período. Embora tal prazo se revele exíguo, levando a medida da interceptação telemática a se afastar da meta de equilíbrio perseguida na busca de eficiência e garantismo, não se pode lançar mão do princípio da proporcionalidade ou de qualquer outro para, aumentando os níveis admitidos por lei para violação de um direito individual, dilatar o prazo de interceptação de comunicações;

24) O prazo de 30 dias, prorrogável uma vez por igual período, se apresentaria como capaz de atender ao subprincípio da exigibilidade temporal e permitir aos sujeitos processuais o exercício adequado de suas faculdades, direitos, garantias e poderes, favorecendo, assim, a aproximação de uma meta de eficiência e garantismo;

25) A fixação de prazos excessivamente dilatados, como seis meses ou um ano, ou mesmo a possibilidade de intermináveis prorrogações, mais se parecem com um simulacro de cumprimento ao subprincípio da exigibilidade temporal do que um efetivo cumprimento. Afinal, em verdade, não importam numa real limitação temporal à medida coativa, mas num modo meramente formal de estabelecer números sem qualquer vinculação a uma razoabilidade;

26) Quanto aos legitimados a autorizar a interceptação, temos que os membros dos Poderes Legislativo e do Executivo, pela própria natureza de suas posições, de seus cargos, a forma pela qual são escolhidos ou nomeados, o ambiente que cerca a troca de interesses políticos – que, diga-se, poderão ser os mais legítimos, lícitos e verdadeiramente representativos de seu eleitorado –, não são dotados dos três elementos essenciais àquele que deve desempenhar o papel de zelador das garantias fundamentais: isenção, imparcialidade e independência. Ademais, a não exigência de formação jurídica para o exercício de seus cargos é outro fator a desqualificá-los para a tarefa de apreciar o cabimento jurídico da restrição de um direito fundamental. Temos, portanto, que, em sendo a interceptação das comunicações telemáticas um meio de obtenção de prova que

depende de uma invasão profunda nos direitos fundamentais do indivíduo, para o que se impõe a atuação de um guardião que ostente os atributos da imparcialidade, independência e isenção, sua implementação está condicionada à cláusula da reserva de jurisdição, não podendo ser determinada por CPI ou, como nas experiências britânica, norte-americana e espanhola, por autoridades do Poder Executivo. Sob outro aspecto, note-se, ainda, que, se um tribunal for instituído ou um juiz nomeado ou transferido especialmente para julgar um determinado caso, ninguém hesitaria em vislumbrar ferimento à regra do juiz natural (art. 5º, XXXVII e LIII, CF). E a própria forma de instalação de uma CPI, totalmente casuística, voltada sempre para investigar um caso específico, nada mais seria do que, por excelência, uma afronta a essa regra que incide na base da atuação jurisdicional. Podemos afirmar, portanto, que os sistemas espanhol, norte-americano e principalmente o britânico destinam, no que se refere às autoridades que podem deferir interceptação de comunicações telemáticas, tratamento que se encontra mais distanciado da meta de eficiência e garantismo do que o brasileiro;

27) O juiz não pode determinar interceptação de comunicações de ofício, tendo em vista que lhe subtrairia a imparcialidade, ofendendo o núcleo essencial de garantias;

28) A não incidência do contraditório na investigação, não prejudica o direito do suspeito de se defender de forma efetiva naquela fase, requerendo os atos investigatórios necessários à sustentação de suas alegações, dentre os quais a interceptação das comunicações de vítimas e testemunhas. Em contrapartida a esse direito, existe, por óbvio, um dever da autoridade que presida a investigação de decidir os requerimentos defensivos de forma motivada, o que poderá ser impugnado através de *habeas corpus* ou, em tempos de restrição exacerbada de seu cabimento, mandado de segurança. Sem o respeito a tal direito defensivo, a balança penderia para o lado da acusação (da futura acusação), tornando-se desiguais as forças das partes (na futura instrução processual) e se quebrando o núcleo essencial de garantias em razão de violação à ampla defesa;

29) O mesmo direito de requerer interceptação deve ser assegurado à vítima ou querelante, na linha do que chamamos de uma significativa tendência legislativa no sentido de aumentar prestígio e as prerrogativas desse personagem no processo penal;

30) No entanto, a interceptação realizada a requerimento de particulares (como o suspeito ou a vítima) não poderá ser implementada por eles próprios, devendo sê-lo pela polícia, impondo-se, no entanto, a previsão de mecanismos que permitam o acompanhamento e a fiscalização da medida por quem tenha requerido a medida. Defesa e vítima, portanto,

têm legitimidade para requerer (mas não para implementar) interceptação de comunicações, devendo haver um procedimento pelo qual o interessado na prova, em sendo um particular, possa acompanhar sua colheita, a ser realizada pela polícia;

31) Tal qual fez a Espanha com seu *Centro Nacional de Inteligencia*, a legislação e a própria Constituição brasileiras deveriam ter permitido à ABIN lançar mão de interceptação de comunicações para o desempenho de seu múnus legal, ainda que para fins não penais, desde que servindo a relevantes interesses nacionais. Afinal, se as experiências inglesa e norte-americana mostraram que seus ordenamentos, em numerosas circunstâncias, afastam o sigilo das comunicações apenas em relação aos estrangeiros, o que inclui os brasileiros, não nos parece razoável colocar o serviço de inteligência brasileiro e o próprio Brasil em franca desigualdade, o que ofende até mesmo o princípio da reciprocidade. Não advogamos, no entanto, a sonegação dos direitos fundamentais aos não residentes no Brasil, mas entendemos que os termos da lei e da Constituição teriam andado melhor se assegurassem a possibilidade de interceptação pela ABIN;

32) A destruição ou inutilização de uma determinada parte do material que se amealhou por meio de interceptação de comunicações constitui uma forma de seleção do que será aproveitado como prova e do que será excluído do processo, o que permite inferir a relevância do ato a se realizar com fulcro no artigo 9º e §único da Lei 9296/96. Diante disso, a prova arrecadada por meio de interceptação de comunicações exige a observância de sua cadeia de custódia com o mesmo nível de cuidado que se exige em relação a vestígios e amostras médico-legais, pois também as comunicações captadas serão únicas e irrepetíveis, devendo, por tal razão, ser preservadas em sua inteireza, em sua forma autêntica e genuína, para, posteriormente, ser amplamente disponibilizadas às partes até o término do processo penal ou até sua regular destruição;

33) Ninguém pode substituir a própria defesa, ou mesmo a acusação, na verificação do que constitui ou não elemento probatório de seu interesse. Diante disso, a indevida seleção ou a irregular destruição de parte do material comunicativo coletado pelo Estado sem a anuência da defesa é causa de imprestabilidade integral do material captado, tendo em vista a quebra da cadeia de custódia, a quebra da confiabilidade do todo probatório, a não preservação da prova em sua forma inteira e genuína;

34) Comparando-se normas que cercam a inutilização de comunicações inservíveis na Itália e no Brasil, aquelas se aproximam mais do ponto de equilíbrio tido como meta de

eficiência e garantismo do que estas. Isto porque, enquanto na Itália a lei prevê que as partes serão ouvidas antes que se inutilizem comunicações interceptadas, no Brasil, a lei sinaliza (com o termo "facultada", do § único, do art. 9º, da Lei 9.296/96) que seria possível se promover a supressão irreversível de fontes de prova, sem que a defesa possa antes avaliar se delas irá se servir. Tal aspecto da lei impede que um dos sujeitos processuais, mais precisamente o acusado, exerça adequadamente suas faculdades, seus direitos, suas garantias, porquanto lhe suprime o direito à prova, violando a ampla defesa e o contraditório, ambos integrantes do núcleo essencial de garantias. Por força do próprio texto constitucional, ao assegurar a ampla defesa e o contraditório, a presença da defesa no ato de inutilização de material interceptado tido por inútil é, portanto, obrigatória, e não facultativa;

35) Quanto ao direito de acesso ao material captado por meio das interceptações, o ordenamento brasileiro permite o exercício das prerrogativas processuais das partes mais adequadamente do que o norte-americano, que somente consente o acesso defensivo ao material em raras circunstâncias, condicionando-o sempre à avaliação do juiz acerca do interesse que a defesa poderia ter no material;

36) Prova ilícita é aquela obtida, admitida ou produzida com violação das garantias constitucionais, sejam as que asseguraram liberdades públicas, sejam as que estabelecem garantias processuais, sendo o desentranhamento mero mecanismo técnico para assegurar uma proibição de sua valoração;

37) Quanto ao tratamento da prova ilícita, a legislação brasileira seguiu mais os parâmetros de eficiência e garantismo, se aproximando mais da meta de ponto médio entre hipergarantismo e repressão a todo custo do que a Inglaterra, que, embora tenha disciplinado hipóteses nas quais o material interceptado deveria ser suprimido, trouxe um extenso rol de exceções a praticamente esvaziar a garantia, notadamente em casos envolvendo terrorismo, imigração e organizações proibidas. Já a legislação dos Estados Unidos contém dispositivos de aparente eficácia, mas que acabam esvaziados em razão da ampla discricionariedade dada aos tribunais no tratamento da ilicitude por derivação, que, a nosso ver, há que ser objetivo e deve ter a inadmissibilidade probatória como regra e o aproveitamento como rara exceção. Em matéria de exame de ilicitude por derivação, a regra deve ser a de que uma ilicitude no curso da investigação contamine todas as provas subsequentes, devendo o aproveitamento destas residir no campo da excepcionalidade, e não o contrário.

38) Se, por um lado, criticamos, no item 4.3, as tentativas vãs de sistematizar ou criar microssistemas normatizadores da valoração de juízos de probabilidade ou verossimilhança e mesmo do dito juízo de certeza necessário para provimentos judiciais finais, já que a palavra final do raciocínio sempre acabará entregue à incontrolável discricionariedade humana, a um autêntico ato de fé, insuscetível de controles técnicos, por outro, entendemos que a análise da ilicitude por derivação pode e deve ser eminentemente objetiva e que o pouco que resta nesse campo para a discricionariedade humana quanto ao exame da relação de causalidade entre a prova ilícita originária e a prova ilícita por derivação deve ter interpretação restritíssima em favor do indivíduo. Afinal, de nada adiantaria uma norma constitucional inadmitindo a prova ilícita, se esta puder ser salva por meio de interpretações tolerantes no uso do *inevitable discovery* e do *independent source*, ou por meio de raciocínios como o *Brown test* norte-americano ou argumentos de que o uso do *Miranda warnings* ao final de uma sequência de atos policiais inaugurada por algum excesso policial criminoso pudesse atenuar ou dissipar a contaminação da ilicitude de origem sobre a prova derivada. Do contrário, estar-se-ia a permitir o expediente que, no item 4.9, chamamos de uma espécie de "lavagem de prova ilícita", expressão que forjamos com o sentido de uma medida intermediária, entre a ilicitude originária e a prova derivada, com fins a dissimular a origem daquela e "dissipar" a ilicitude;

39) Ainda que a defesa técnica não possa atuar durante uma interceptação em andamento, porquanto sigilosa, ela deve ter meios de, ao exercer o contraditório diferido, compreender e fiscalizar a exata origem de cada elemento probatório surgido nos autos, sua rastreabilidade, sob pena de ofensa ao núcleo essencial de garantias, precisamente em seus componentes ampla defesa e contraditório;

40) Quanto ao encontro fortuito de provas, se, em matéria de interceptação de comunicações, o bem jurídico em jogo será o direito à inviolabilidade do sigilo das comunicações, e junto com ele a intimidade e a privacidade das pessoas monitoradas, todos direitos constitucionais fundamentais protetores de liberdades públicas, está claro que eles não podem sofrer restrição indevida, ilegal ou desproporcional, sob pena de inquinar de ilícita a prova decorrente da referida violação. Neste campo, portanto, ou a prova será lícita, e aí com plena condição de gerar efeitos, ou será ilícita e, nesse caso, absolutamente inadmissível para qualquer fim. Diante disso, não nos parece adequado o tratamento dualista da prova fortuitamente encontrada. É que ou ela será lícita, podendo

gerar efeitos jurídicos, ou será ilícita e, nesse caso, não poderá ser admitida para nenhum fim, nem como notícia de crime, nem como fonte de prova para nova investigação, sob pena de se estar concebendo um raciocínio contraditório e frontalmente violador da vedação constitucional às provas ilícitas (art. 5º, LVI) e até mesmo do artigo 157 do CPP;

41) Para se definir o que tornará a prova fortuitamente encontrada lícita e admissível ou, ao contrário, ilícita e inadmissível, adotamos o critério da previsibilidade que a lei deve dar ao indivíduo acerca das consequências de seus atos. Nesse sentido, por força de convenções internacionais de direitos humanos, na interpretação que lhes deram as cortes internacionais de direitos humanos[769], eventual medida que afaste o sigilo das comunicações precisa estar expressamente prevista na lei, em norma acessível a todos, mediante os meios de publicação, e prevendo, com clareza e precisão, as condições pelas quais os poderes públicos estarão autorizados a adotar a medida de interceptação. Diante disso, a prova fortuitamente encontrada só terá validade se o crime que ela revelar for daqueles que admita interceptação, independentemente de nexo causal ou de conexão com o crime que ensejou a medida. Caso não reste atendido esse pressuposto, a prova não poderá ser utilizada para nenhuma finalidade, nem mesmo como notícia de crime ou fonte de prova para nova investigação;

42) A modalidade comunicativa conhecida como grupo de bate-papo ou *chat* pode gerar a peculiar situação de que uma autorização de monitoramento seja implementada num momento em que já haja, naquele mesmo veículo de comunicação, e agora ao acesso do investigador, registros de diversas comunicações pretéritas. A nosso ver, a hipótese constitui exemplo clássico de encontro fortuito de provas, mas aqui a solução deve ser diversa da adotada acima. Em tal situação, deve-se zelar pelo subprincípio da exigibilidade temporal, de modo que, se a interceptação de uma comunicação realizada por meio de *chat* foi regularmente autorizada em determinado dia, para perdurar por prazo determinado, com data de início definida, os registros de diálogos pretéritos, tenham eles emanado do próprio investigado ou de outros participantes, não poderão ser aproveitados para nenhuma finalidade, sob pena de a interceptação se transfigurar numa violação ao direito ao sigilo das comunicações sem nenhum limite de tempo;

43) Diferentemente do que ocorre nos Estados Unidos e na Inglaterra, no Brasil, não é possível interceptar comunicações com fins a prevenir um crime, não em razão de

[769] Ver item 1.3.

vedação constitucional, mas sim em respeito à ausência de concepção infraconstitucional de uma investigação criminal relativa a crime futuro. Enquanto pendente eventual lei ordinária neste sentido, e aí não havendo previsão de investigação relativa a crime futuro, eventual ato de promover interceptação preventiva afrontaria a exigência, recorrente nas cortes internacionais, de que a lei preveja a medida, de forma clara e precisa. Isto, no entanto, não afastaria que, em situações limites, para salvar vidas ou proteger outro bem jurídico de altíssima relevância, incidisse causa excludente de ilicitude em caso de interceptação não autorizada;

44) Embora o legislador brasileiro não tenha regulamentado o uso de criptografia, o Projeto de Lei nº 5.285/2009, da Câmara dos Deputados, busca exigir que as chaves de violação de criptografias sejam previamente depositadas pelos fabricantes na ANATEL e criminalizar o uso não autorizado da tecnologia. A medida equivaleria a exigir que cada cidadão deixasse a porta de sua residência destrancada ou que fornecesse uma cópia da chave ao Estado, de modo a facilitar-lhe o ingresso. Mas, assim como a porta trancada não tem a finalidade única de dificultar o ingresso das forças do Estado, servindo também para afugentar a ação de invasores de toda sorte, a criptografia nas comunicações também se presta a proteger segredos das mais diversas espécies, atinentes desde os assuntos relativos à vida privada de cada um até os segredos industriais, financeiros e até de Estado. O direito do cidadão de usar meios adicionais para proteger o sigilo de suas próprias comunicações, como a criptografia, está compreendido no âmbito de proteção do direito ao sigilo das comunicações. Afinal, pelo critério da especificidade, temos que o uso de criptografia se mostra um ato específico do exercício do direito à inviolabilidade do sigilo das comunicações, e não uma circunstância meramente acidental de seu exercício. Mais do que uma ação estruturalmente necessária ao exercício do direito ao sigilo das comunicações, entendemos que aquele que instala um sistema de criptografia para proteger suas comunicações está praticando um ato inerente ao próprio direito fundamental. A proibição generalizada e irrestrita do uso de criptografia, como pretende o referido Projeto, atenderia o subprincípio da adequação, porquanto é apta a obter, mais comodamente, o fim pretendido pelo interesse público persecutório, mas não atenderia os dois outros subprincípios do princípio da proporcionalidade, quais sejam, o da exigibilidade e o da proporcionalidade em sentido estrito. O da exigibilidade restaria desatendido porque o Estado estaria lançando mão de um meio nada comedido

(exigibilidade material), sem a mínima limitação em seu âmbito de intervenção (exigibilidade espacial) e sem que os sacrifícios impostos se restringissem somente à pessoa do imputado (exigibilidade pessoal). A proporcionalidade em sentido estrito, por sua vez, restaria desatendida porquanto não haveria equilíbrio entre as vantagens do fim (facilitação na interceptação das comunicações daquela pequena parcela da população que o Estado necessite monitorar) e as desvantagens do meio, incidentes sobre tudo e todos, de modo a fragilizar o direito ao sigilo das comunicações de um número indeterminado de pessoas.

REFERÊNCIAS[770]

AFONSO, Orlando Viegas Martins. **Poder Judicial**: independência in dependência. Coimbra: Livraria Almedina, 2004.

AGUILAR, Francisco. **Dos conhecimentos fortuitos obtidos através de escutas telefônicas**. Coimbra: Almedina, 2004.

ALEXY, Robert. **Teoria dos direitos fundamentais**. Tradução Virgílio Afonso da Silva. 2ª ed. São Paulo: Malheiros, 2011.

ALMEIDA, Joaquim Canuto Mendes de. **Princípios fundamentais do processo penal**. São Paulo: Revista dos Tribunais, 1973.

ANDRADE, Manuel da Costa. Das escutas telefônicas. In: SILVA, Marco Antonio da (Coord.). **Direito penal especial, processo penal e direitos fundamentais**: visão luso-brasileira. São Paulo: Quartier Latin do Brasil, 2006.

ANTONIO, Ángel Luis Alonso de; ANTONIO, José Antonio Alonso de. **Derecho constitucional español**. 4ª ed. Madrid: Editorial Universitas S.A., 2006.

AROCA. Juan Montero. **La intervención de las comunicaciones en el proceso penal**: un estudio jurisprudencial. Valencia: Tirant lo Blanch, 1999.

AVOLIO, Luiz Francisco Torquato. **Provas ilícitas**: interceptações telefônicas, ambientais e gravações ambientais. 4ª ed. São Paulo: Revista dos Tribunais, 2010.

BADARÓ, Gustavo Henrique Righi Ivahy. Interceptação de comunicações telefônicas e telemáticas: limites ante o avanço da tecnologia. In: LIMA, José Corrêa de; CASARA, R. R. Rubens. (Coord.). **Temas para uma perspectiva crítica do direito**: homenagem ao Professor Geraldo Prado. Rio de Janeiro: Lumen Juris, 2010, p. 483-499.

_____. **Ônus da prova no processo penal**. São Paulo: Revista dos Tribunais, 2003.

_____. **Processo penal**. Rio de Janeiro: Elsevier, 2012.

BALL, James; BORGER, Julian; GREENWALD, Glenn. Revealed: how US and UK spy agencies defeat internet privacy and security. **The Guardian**. 06 set. 2013. Disponível em: <http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security>. Acesso em: 29 set. 2013.

[770] Segundo a norma NBR 6023 da ABNT.

BARBOSA, Rui. Discursos parlamentares: sessão de 05 de agosto de 1905 do Senado Federal. In: NERY, Fernando (Org.). **Obras completas de Rui Barbosa**, v. XXXII, tomo I, Rio de Janeiro: Ministério da Educação e Cultura, 1955.

BARROS, Romeu Pires de Campos. **Processo penal cautelar**. Rio de Janeiro: Forense, 1982.

BARROSO, Luís Roberto. **Curso de direito constitucional contemporâneo**: os conceitos fundamentais e a construção do novo modelo. São Paulo: Saraiva, 2009.

BASTERRA, Marcela I. Prueba y médios de comunicación: la cuestión constitucional. In: ARAZI, Roland. (Org.). **Prueba ilícita y prueba científica**. Santa Fe, Argentina: Rubinzal-Culzoni Editores, 2008.

BASTOS, Celso Ribeiro. **Curso de direito constitucional**. 22ª ed., rev. e atual. por Samantha Meyer-Pflug. São Paulo: Malheiros, 2010.

BEDAQUE, José Roberto dos Santos. **Tutela cautelar e tutela antecipada**: tutelas sumárias e de urgência (tentativa de sistematização). São Paulo: Malheiros, 1998.

BIANCHINI, Alice. **Falta de delegacias especializadas**: outra forma de violência contra a mulher. Disponível em: <http://ww3.lfg.com.br/public_html/article.php?story=201103151453246&mode=print>. Acesso em: 03 jan. 2014.

BITTAR, Carlos Alberto. **Os direitos da personalidade**. 5ª ed., Rio de Janeiro: Forense Universitária, 2001.

BRASIL. Câmara dos Deputados. Projeto de Lei nº 5.285/2009, apresentado em 27.05.2009, pela comissão parlamentar de inquérito instaurada com a finalidade de investigar escutas telefônicas clandestinas/ilegais, conforme denúncia publicada na Revista "Veja", edição 2022, nº 33, de 22 de agosto de 2007. Disponível em: <http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=436096>. Acesso em: 05 jan. 2014.

_____. Câmara dos Deputados. Projeto de Lei nº 3.514/1989. Autor Deputado Miro Teixeira. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=55F3499F5ADD4FBB2DCEB356B0FF8DC7.node2?codteor=1155030&filename=Avulso+-PL+3514/1989>. Acesso em: 22 dez. 2013.

_____. Tribunal de Justiça do Estado do Rio de Janeiro. Juizados Especiais: enunciados e recomendações do PJERJ. Ato TJ nº SN12, de 23.06.2010. Disponível em: <http://portaltj.tjrj.jus.br/documents/10136/30422/juizados-especiais.pdf>. Acesso em: 11.12.2013.

_____. Parecer nº 1.636, de 2010, estabelecendo a redação final do Projeto de Lei do Senado nº 156, de 2009. Disponível em:

<http://www.senado.gov.br/atividade/materia/getPDF.asp?t=85509&tp=1>. Acesso em: 01 jun. 2013.

_____. Senado Federal. SF RQS 1224/2004 de 14.09.2004. Autor: Senador Arthur Virgílio. Disponível em: < http://www.senado.gov.br/atividade/materia/detalhes.asp?p_cod_mate=70061>. Acesso em: 06 jan. 2014.

_____. Senado Federal. SF RRE 68/2013 de 08.08.2013. Autor: Senador Ricardo Ferraço. Disponível em: <http://www.senado.gov.br/atividade/materia/detalhes.asp?p_cod_mate=113884>. Acesso em: 06 jan. 2014.

_____. Superior Tribunal de Justiça. HC 113477/DF, rel. min. Maria Thereza de Assis Moura, 6ª T., j. 20.03.2012, DJe 16.04.2012.

_____. Superior Tribunal de Justiça. HC 144378/DF, rel. min. Laurita Vaz, 5ª T., j. 22.11.2011, DJe 02.12.2011.

_____. Superior Tribunal de Justiça. HC 171910/SP, rel. min. Maria Thereza de Assis, 6ª T., j. 21.11.2013, DJe 09/12/2013.

_____. Superior Tribunal de Justiça. HC 212643/PE, rel. min. Sebastião Reis Júnior, 6ª T., j. 06.03/2012, DJe 26.03.2012.

_____. Superior Tribunal de Justiça. HC 263985/SP, rel. min. Marco Aurélio Bellizze, 5ª T., j. 19.11.2013, DJe 25.11.2013.

_____. Superior Tribunal de Justiça. HC 76686/PR, rel. min. Nilson Naves, 6ª T., j. 09.09.2008, DJe 10.11.2008.

_____. Superior Tribunal de Justiça. RHC 13274/RS, rel. min. Gilson Dipp, 5ª T., j. 19.08.2003, DJ 29.09.2003.

_____. Superior Tribunal de Justiça. RMS 28284/RJ, rel. Napoleão Nunes Maia Filho, 5ª T., j. 04.12.2009, DJe 22.02.2010.

_____. Supremo Tribunal Federal. ADI 1570-2, rel. min. Maurício Corrêa, Pleno, j. 12.02.2004, DJ 22.10.2004.

_____. Supremo Tribunal Federal. HC 107521/PR, rel. min. Dias Toffoli, 1ª T., j. 19.02.2013, DJe 22.03.2013.

_____. Supremo Tribunal Federal. HC 109956/PR. rel. min. Marco Aurélio, 1ª T., j. 14.08.2012, DJ 11.09.2012.

_____. Supremo Tribunal Federal. HC 69912/RS, rel. min. Sepúlveda Pertence, Pleno, j. 16.12.1993, DJ 25.03.1994.

_____. Supremo Tribunal Federal. HC 70814, rel. min. Celso de Mello, j. 01.03.1994, DJ 24.06.1994.

_____. Supremo Tribunal Federal. HC 72588/PB, rel. min. Maurício Corrêa, Pleno, j. 08.11.1995, DJ 04.08.2000.

_____. Supremo Tribunal Federal. HC 74116/SP, rel. min. Néri da Silveira, rel. p/ acórdão min. Maurício Corrêa, 2ª T, j. 05.11.1996, DJ 14.03.1997.

_____. Supremo Tribunal Federal. HC 80949/RJ, rel. min. Sepúlveda Pertence, 1ª T., j. 30.10.2001, DJ 14.12.2001

_____. Supremo Tribunal Federal. HC 83515/RS, Pleno, rel. min. Nelson Jobim, j. 16.09.2004, DJ 04.03.2005.

_____. Supremo Tribunal Federal. MS 23452/RJ, rel. min. Celso de Mello, j. 16.09.1999, DJ 12.05.2000.

_____. Supremo Tribunal Federal. Pet-QO 577/DF, rel. min. Carlos Velloso, Pleno, j. 25.03.1992, DJ 23.04.1993.

_____. Supremo Tribunal Federal. RHC 117467/SP, 1ª T., rel. min. Dias Toffoli, j. 05.11.2013, DJe 22.11.2013.

_____. Supremo Tribunal Federal. RHC 85575/SP, rel. min. Joaquim Barbosa, 2ª T., j. 28.03.2006, DJ 16.03.2007.

_____. Supremo Tribunal Federal. Súmula Vinculante nº 14. Pleno. Aprovada na sessão de 02.02.2009.

BUCHANAN, Matt. How the N.S.A. Cracked the Web. **The New Yorker**. 07 set. 2013. Disponível em: <http://www.newyorker.com/online/blogs/elements/2013/09/the-nsa-versus-encryption.html>. Acesso em: 06 ago. 2013.

BUCHSBAUM, Paulo Eduardo Laurenz. **Texto de Criptografia e "Tim Tim"** [mensagem pessoal]. Mensagem recebida por <sidi@ffernandes.adv.br> em 29 set. 2013.

CADY, Spencer. S. Reconciling privacy with progress: Fourth Amendment protection of e-mail stored with and sent through a third-party internet service provider. **Drake Law Review**, 61 Drake L. Rev. 225, 2012.

CAETANO, Marcello. **Manual de direito administrativo**. Tomo I. 10ª ed. Coimbra: Livraria Almedina, 1982.

CALAMANDREI, Piero. **Introduzione allo studio sistematico dei provvedimenti cautelari**. Opere giuridiche. v. IX. Napoli: Morano, 1983.

_____. Verità e verosimiglianza nel processo civile. In: **Rivista di Diritto Processuale**, p. 164/192, Milano: Giuffrè, 1955.

CALMON, Alberto. **Le intercettazioni nel processo penale**. Milano: Giuffrè, 1996.

CAMPOS, Federico. La relevancia de la custodia de la evidencia en la investigación judicial. **Medicina Legal de Costa Rica**, v. 19, nº 1, Heredia mar. 2002. Disponível em: <http://www.scielo.sa.cr/scielo.php?script=sci_arttext&pid=S1409-00152002000100008&lng=es&nrm=iso>. Acesso em: 04 jan. 2014.

CANOTILHO, José Joaquim Gomes. **Direito constitucional e teoria da Constituição**. 7ª ed. Coimbra: Almedina, 2000.

CARNELUTTI, Francesco. **A prova civil**. Tradução Lisa Pary Scarpa. Campinas: Bookseller, 2001.

CASA DO DETETIVE. Disponível em: <http://casadodetetive.com.br/interceptor-multiband-dispositivo-decifracao-p-436.lgz?osCsid=a0e9225248672a8937d67220b521bf45>. Acesso em: 23 set. 2013.

CASARA, Rubens R. R. Juiz das garantias: entre uma missão de liberdade e o contexto de repressão. In: COUTINHO, Jacinto Nelson de Miranda; CARVALHO, Luis Gostavo Grandinetti Castanho de. (Org.). **O novo processo penal à luz da Constituição**: análise crítica do Projeto de Lei nº 156/2009, do Senado Federal. Rio de Janeiro: Lumen Juris, 2010.

CHIOVENDA. Giuseppe. **Principii di diritto processuale civile**. 3ª ed. Napoli: Jovene, 1965.

CLUBE DO HARDWARE. Desenvolvido por Gabriel Torres. Disponível em: <http://www.clubedohardware.com.br>. Acesso em: 25 ago. 2013.

CONDEIXA, Fábio de Macedo Soares Pires. Interceptações das comunicações de estrangeiros não residentes: Wiretapping of non-resident aliens. In: **Programa de Estudos em Criminologia e Ciências Penitenciárias – PROCRIM**, São Paulo, ano 3, nº 04, dezembro/2013/ferereiro/2014.

COPELIOVITCH, Marcelo. **Re: Gold Lock - Secure Call To Any Phone Number** [menssagem pessoal]. Mensagem recebida por sidi@ffernandes.adv.br em 09 set. 2013.

CORNELL UNIVERSITY LAW SCHOOL. Legal Information Institute. Ithaca, NY. Disponível em: <http://www.law.cornell.edu>. Acesso em: 02 fev. 2013.

CORTE INTERAMERICANA DE DIREITOS HUMANOS. Caso Atala Riffo y Niñas vs. Chile. Disponível em: <http://www.corteidh.or.cr/docs/casos/articulos/seriec_239_esp.doc>. Acesso em: 14 jul. 2012.

_____. Caso Escher e outros vs. Brasil. Disponível em: <http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf>. Acesso em 14 jul. 2012.

COSTA JR., Paulo José da. **O direito de estar só**: tutela penal da intimidade. 4ª ed. rev. e atual. São Paulo: Revista dos Tribunais, 2007.

COSTA, Helena Regina Lobo da; LEONARDI, Marcel. Busca e apreensão e acesso remoto a dados em servidores. In: **Revista Brasileira de Ciências Criminais**, São Paulo, v. 19, n. 88, p. 203-223, jan./fev. 2011.

CURTIS, George E. **The law of cybercrime and their investigations**. Boca Raton: CRC Press, Taylor and Francis Group, 2012.

DAHRENDORF, Ralph G. et al. (Ed.) The Interception of Communications Act. In: **The Modern Law Review**. vol. 49, n. 1. London: Stevens & Sons Limited, 1986. Disponível em: <http://heinonline.org/HOL/Page?handle=hein.journals/modlr49&div=2&collection=journals&set_as_cursor=0&men_tab=srchresults&terms=the modern law review|49&type=matchall#102>. Acesso em: 16 abr. 2013.

DAMASKA, Mirjan Radovan, **Evidentiary Barriers to Conviction and Two Models of Criminal Procedure**: A Comparative Study. Faculty Scholarship Series. Paper 1591, 1973.

DAVENPORT, Justin. Tens of thousands of CCTV cameras, yet 80% of crime unsolved. **London Evening Standard**. 19 set. 2009. Disponível em: <http://www.standard.co.uk/news/tens-of-thousands-of-cctv-cameras-yet-80-of-crime-unsolved-6684359.html>. Acesso em 23 out. 2013.

DELMANTO, Roberto; DELMANTO JR., Roberto. A permissão constitucional e a nova lei de interceptação telefônica. **Boletim do Instituto Brasileiro de Ciências Criminais**, São Paulo, n. 47, p. 2, out. 1996.

DEZEM, Guilherme Madeira. **Da prova penal:** tipo processual, provas típicas e atípicas (atualizado de acordo com as Leis 11.689, 11.690 e 11.719/08). Campinas: Millennium Editora, 2008.

DÍGITRO. Disponível em: <http://www.digitro.com.br/pt/>. Acesso em: 26 ago. 2013.

DOSTOIEVSKI, Fedor M. **Recordação da casa dos mortos**. Tradução Geraldo Vieira. São Paulo: Saraiva, 1949.

DOTTI, René Ariel. A liberdade e o direito à intimidade. In: **Revista de Informação Legislativa**, Brasília, ano 17, nº 66, p. 125-152, abr./jun. 1980.

DURANTE, Gabriel Barros. **Redes Peer-to-Peer**. Universidade Federal do Rio de Janeiro. Departamento de Engenharia Eletrônica e de Computação Disciplina: Redes de Computadores I. Professor: Otto Carlos M. B. Duarte. Disponível em: <http://www.gta.ufrj.br/grad/04_1/p2p/>. Acesso em: 02 out. 2013.

ENCYCLOPÆDIA BRITANNICA. Disponível em: <http://global.britannica.com/>. Acesso em: 12 set. 2013.

ESPANHA. Agencia Española de Protección de Datos, Nota de Prensa. 19 jan. 2010. Disponível em: <https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2010/notas_prensa/common/enero/190110_np_previo_dia_europeo_2010.pdf>. Acesso em: 05 abr. 2013.

_____. Congreso de los Diputados. Disponível em: <http://www.congreso.es>. Acesso em: 03 jun. 2013.

_____. Gobierno de España. Ministerio de la Presidencia. Agencia Estatal Boletín Oficial del Estado. Disponível em: <http://www.boe.es/>. Acesso em: 27 mai. 2013.

_____. TOURÓN, C. C. P. Memoria elevada al gobierno de s. m. presentada al inicio del año judicial por el Fiscal General del Estado, v. 1. Imprenta Nacional del Boletín Oficial del Estado, Madrid, 2010.

_____. Tribunal Constitucional de España. Sala Primera. Recurso de amparo 5546/1999. Sentencia 123/2002. Fecha 20/05/2002. Disponível em: <http://hj.tribunalconstitucional.es/HJ/pt/Resolucion/Show/4659>. Acesso em 30 mai. 2013.

_____. Tribunal Constitucional de España. Sala Primera. Recurso de amparo 1829-2003. Sentencia 281/2006. Fecha 09/10/2006. Disponível em: <http://hj.tribunalconstitucional.es/HJ/pt/Resolucion/Show/5883>. Acesso em: 30 mai. 2013.

_____. Tribunal Constitucional de España. Sala Primera. Recurso de amparo 6409-2004. Sentencia 230/2007. Fecha 05/11/2007. Disponível em: <http://hj.tribunalconstitucional.es/HJ/pt/Resolucion/Show/6197>. Acesso em: 29 mai. 2013.

_____. Tribunal Constitucional de España. Sala Primera. Recurso de amparo 3787-2001. Sentencia 70/2002. Fecha 03/04/2002. Disponível em: <http://hj.tribunalconstitucional.es/HJ/pt/Resolucion/Show/4606>. Acesso em: 30 mai. 2013.

_____. Tribunal Constitucional de España. Sala Segunda. Recurso de amparo 167/1983. Sentencia 114/1984. Fecha 29/11/1984. disponível em: <http://hj.tribunalconstitucional.es/HJ/pt-BR/Resolucion/Show/SENTENCIA/1984/114>. Acesso em: 30 mai. 2013.

_____. Tribunal Supremo. Sala de lo Penal. STS 1550/2010. Recurso casación nº 121/2009. Resolución 247/2010. 28079120012010100231. Disponível em: <http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=TS&refere

nce=5554451&links=informaticos&optimize=20100422&publicinterface=true>. Acesso em: 29 mai. 2013.

_____. Tribunal Supremo. Sala de lo Penal. STS 2756/2008. Recurso 10983/2007. Resolución 249/2008. 28079120012008100290. Ponente: Manuel Marchena Gomez. Fecha: 20/05/2008. Disponível em: <http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=TS&reference=54594&links=&optimize=20080626&publicinterface=true>. Acesso em: 29 mai. 2013.

_____. Tribunal Supremo. Sala de lo Penal. STS 5606/2010, Recurso Casación nº 621/2010. Resolución 895/2010. 28079120012010100841. Disponível em: <http://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=TS&reference=5781704&links=&optimize=20101118&publicinterface=true>. Acesso em: 29 mai. 2013.

ESPIONAGEM é afronta, diz Dilma na ONU: Na abertura da 68ª Assembleia Geral presidenta ressaltou que interceptações ferem o direito internacional e a soberania dos países. **Carta Capital**. 24 set. 2013. Disponível em: <http://www.cartacapital.com.br/politica/201cjamais-pode-uma-soberania-firmar-se-em-detrimento-de-outra201d-diz-dilma-sobre-espionagem-6642.html>. Acesso em: 30 set. 2013.

ESTADOS UNIDOS DA AMÉRICA. Court of Appeals of Maryland. Jody Lee Miles v. State of Maryland. 365 Md. 488; 781 A.2d 787; 2001 Md. LEXIS 614. Disponível em: <http://www.lexisnexis.com/hottopics/lnacademic/?>. Acesso em: 12 fev. 2013.

_____. Supreme Court of the United States. Brown v. Illinois. 422 U.S. 590; 95 S. Ct. 2254; 45 L. Ed. 2d 416; 1975 U.S. LEXIS 82. Disponível em: <http://www.lexisnexis.com/hottopics/lnacademic/?>. Acesso em: 02 mar. 2013.

_____. Supreme Court of the United States. Katz v. United States. 389 U.S. 347; 88 S. Ct. 507; 19 L. Ed. 2d 576; 1967. Disponível em: <http://www.lexisnexis.com/hottopics/lnacademic/?>. Acesso em: 13 fev. 2013.

_____. Supreme Court of the United States. Smith v. Maryland. 442 U.S. 735; 99 S. Ct. 2577; 61 L. Ed. 2d 220; 1979 U.S. Disponível em: <http://www.lexisnexis.com/hottopics/lnacademic/?>. Acesso em: 01 mar. 2013.

_____. Supreme Court of the United States. United States v. Knotts. 460 U.S. 276; 103 S. Ct. 1081. Disponível em: <http://www.lexisnexis.com/hottopics/lnacademic/?>. Acesso em: 01 mar. 2013.

_____. United States Court of Appeals for the Ninth Circuit. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002). Disponível em: <http://www.lexisnexis.com/hottopics/lnacademic/?>. Acesso em: 15 fev. 2013.

_____. United States Court of Appeals for the Eleventh Circuit. United States v. Steiger. 318 F.3d 1039, 1050-52 (11th Cir. 2003). Disponível em: <http://www.lexisnexis.com/hottopics/lnacademic/?>. Acesso em: 12 fev. 2013.

_____. Court of Appeals for the Fifth Circuit. Cressman v. Ellis. 77 Fed. Appx. 744; 2003 U.S. Disponível em: <http://www.lexisnexis.com/hottopics/lnacademic/?>. Acesso em: 13 fev. 2013.

_____. United States Court of Appeals for the Fifth Circuit. Fannie Garcia v. City of Laredo, Texas. 702 F.3d 788; 2012 U.S. App. LEXIS 25370. Disponível em: <http://www.lexisnexis.com/hottopics/lnacademic/?>. Acesso em: 17 fev. 2013.

_____. United States Court of Appeals for the First Circuit. United States v. Larios. 593 F.3d 82; 2010 U.S. Disponível em: <http://www.lexisnexis.com/hottopics/lnacademic/?>. Acesso em: 13 fev. 2013.

_____. United States Court of Appeals for the Fourth Circuit. United States v. Appelbaum. 2013 U.S. App. LEXIS 1746; 41 Media L. Rep. 1177. Disponível em: <http://www.lexisnexis.com/hottopics/lnacademic/?.> Acesso em: 02 mar 2013.

_____. United States Court of Appeals for the Ninth Circuit. Price v. Turner. 260 F.3d 1144, 1147-48 (9th Cir. 2001). Disponível em: <http://www.lexisnexis.com/hottopics/lnacademic/?>. Acesso em: 25 fev. 2013.

_____. United States Court of Appeals for the Sixth Circuit. United States v. Warshak. 631 F.3d 266; 2010 U.S. App. Disponível em: <http://www.lexisnexis.com/hottopics/lnacademic/?>. Acesso em: 27 fev. 2013.

_____. United States District Court for the District of Columbia. United States v. Jones. 451 F.Supp.2d 71, 75, D.D.C. 2006. Disponível em: <http://www.lexisnexis.com/hottopics/lnacademic/?>. Acesso em: 17 fev. 2013.

_____. United States District Court for the District of Utah. United States v. Jones. 364 F. Supp.2d 1303, 1308-09 (D.Utah 2005). Disponível em: <http://www.lexisnexis.com/hottopics/lnacademic/?>. Acesso em: 12 fev. 2013.

_____. United States District Court, Southern District of New York. Application for an order authorizing the interception of oral communications, by Jonathan Kolodner (Assistant United States Attorney). 03 set. 2003. Disponível em: <http://www.politechbot.com/docs/fbi.ardito.affidavit.p1.120106.pdf>. Acesso em: 25 set. 2013.

_____. United States District Court, Southern District of New York. United States of America v. John Tomero et al., No. S2 06 Crim. 0008(LAK). Nov. 27, 2006. Memorandum opinion by Lewis A. Kaplan, District Judge. Disponível em: <http://www.politechbot.com/docs/fbi.ardito.roving.bug.opinion.120106.txt>. Acesso em: 25 set. 2013.

_____. U.S. Government Printing Office. Public Law 107-56-Oct. 26, 2001, Uniting and strengthening america by providing appropriate tools required to intercept and obstruct terrorism (USA Patriot Act) act of 2001. Disponivel em: <http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf>. Acesso em: 16 fev. 2013

EVANS, Ian. Report: London no safer for all its CCTV cameras. **The Christian Science Monitor**. 22 fev. 2012. Disponível em: <http://www.csmonitor.com/World/Europe/2012/0222/Report-London-no-safer-for-all-its-CCTV-cameras>. Acesso em: 18 set. 2013.

EWING, Keith. D. **The Human Rights Act and parliamentary democracy**. Disponível em: <http://onlinelibrary.wiley.com/doi/10.1111/1468-2230.00192/pdf>. Acesso em: 02 jun. 2013.

EXPLANATORY Report of the Convention on Cybercrime of the Concil of Europe. Disponível em: <http://conventions.coe.int/treaty/en/reports/html/185.htm>. Acesso em: 29 jan. 2012.

FERNANDES, Antonio Scarance. O equilíbrio entre a eficiência e o garantismo e o crime organizado. In: **Revista Brasileira de Ciências Criminais**, São Paulo, v. 16, n. 70, p. 226-266, jan./fev. 2008.

_____. Reflexões sobre as noções de eficiência e de garantismo no processo penal. In: _____; ALMEIDA, José Raúl Gavião de; MORAES, Maurício Zanoide de (Coord.). **Sigilo no processo penal**. São Paulo: Revista dos Tribunais, 2008.

_____. O equilíbrio na repressão ao crime organizado. In: _____; ALMEIDA, José Raúl Gavião de; MORAES, Maurício Zanoide de (Coord.). **Crime organizado**: aspectos processuais. São Paulo: Revista dos Tribunais, 2009.

_____. **Processo penal constitucional**. 6ª. ed. São Paulo: Revista dos Tribunais, 2010.

FERRAJOLI, Luigi. **Derecho y razón**: teoria del garantismo penal. 2ª ed. Tradução Perfecto Andrés Ibáñez et al. Madri: Trotta, 1997.

FERRAZ JR., Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista da Faculdade de Direito da Universidade de São Paulo**, São Paulo, v. 88, p. 439-459, jan./dez. 1993.

GABRIEL, Maria Madalena; LOPES, M; BARETA, G. M. S. **Cadeia de Custódia:** uma abordagem preliminar. 2006. Disponível em: <http://ojs.c3sl.ufpr.br/ojs2/index.php/academica/article/view/9022/6315>. Acesso em: 04 jan. 2014.

GARCÍA, Oscar Morales. Seguridad en las redes telemáticas de comunicaciones: la tensión libertad versus control en la política criminal internacional. In: DA AGRA, Cândido et al.

(Org.). **La seguridad en la sociedad del riesgo**: un debate aberto, p. 137-153. Madrid: Atelier, 2003.

GELLMAN, Barton; POITRAS, Laura. U.S., British intelligence mining data from nine U.S. internet companies in broad secret program. **The Washington Post**. 06 jun. 2013. Disponível em: <http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html>. Acesso em: 15 set. 2013.

GILLESPIE, Alisdair. **The English Legal System**. Oxford: Oxford University Press, 2007.

GOMES FILHO, Antonio Magalhães. **Direito à prova no processo penal**. São Paulo: Revista dos Tribunais, 1997.

_____. Provas: Lei 11.690, de 09.06.2008 In: MOURA, Maria Thereza Rocha de (Coord.). **As reformas no processo penal**: as novas leis de 2008 e os projetos de reforma, p. 246/297, São Paulo, Revista dos Tribunais, 2008.

GOMES, Luiz Flavio. Interceptação telefônica e "encontro fortuito" de outros fatos. In: **Boletim do Instituto Brasileiro de Ciências Criminais**, São Paulo, n. 51, p. 6, fev. 1997.

_____; CERVINI, Raúl. **Interceptação telefônica**: Lei 9.296, de 24.07.96 - sigilo das comunicações - limites da inviolabilidade - comunicações telefônicas/telemáticas. São Paulo: Revista dos Tribunais, 1997.

GONÇALVES, Luiz Carlos dos Santos. **Poderes de investigação das comissões parlamentares de inquérito**. São Paulo: Editora Juarez de Oliveira, 2001.

GRECO FILHO, Vicente. **Interceptação telefônica**: considerações sobre a Lei n. 9.296, de 24 de julho de 1996. 2ª ed. rev., atual. e ampl. (com a colaboração de João Daniel Rassi). São Paulo: Saraiva, 2005.

_____. **Interceptação telefônica**: considerações sobre a Lei n. 9.296, de 24 de julho de 1996. São Paulo: Saraiva, 1996.

_____. **Manual de processo penal**. 7ª ed., São Paulo: Saraiva, 2009.

GREEN, Matthew. On the NSA. **A Few Thoughts on Cryptographic Engineering** (blog). 05 set. 2013. Disponível em: <http://blog.cryptographyengineering.com/2013/09/on-nsa.html>. Acesso em: 25 set. 2013.

GREGO, Maurício. O mais poderoso supercomputador do mundo agora é chinês. **Revista Exame**. 17 jun. 2013. Disponível em: <http://exame.abril.com.br/tecnologia/noticias/o-mais-poderoso-supercomputador-do-mundo-agora-e-chines>. Acesso em 23 set. 2013.

GRINOVER, Ada Pellegrini. A iniciativa instrutória do juiz no processo penal acusatório**.** In: **Revista Brasileira de Ciências Criminais**, São Paulo, ano 7, nº 27, jul-set 1999, Revista dos Tribunais, 1999.

_____. Interceptações telefônicas e gravações clandestinas no processo penal. In: **Novas tendências do direito processual de acordo com a Constituição de 1988**. 2ª ed. Rio de Janeiro: Forense Universitária, 1990.

_____. Parecer preferido em 03.12.2009, juntado aos autos do HC 160.662/RJ, em trâmite no Superior Tribunal de Justiça, ainda pendente de julgamento.

_____. **Procedimentos sumários em matéria penal. O processo em evolução**. Rio de Janeiro: Forense Universitária, 1996.

_____; GOMES FILHO, Antonio Magalhaes; FERNANDES, Antonio Scarance. **As nulidades no processo penal**. 11ª ed. São Paulo: Revista dos Tribunais, 2009.

HALLETT, Lawrie. The Space Between: Making room for Community Radio. In: GORDON, Janey (Ed.) **Notions Of Community**: A Collection of Community Media Debates and Dilemmas. Bern: International Academic Publishers, 2008.

HOCHHEISER, Sheldon. **Stars**: Electromechanical telephone switching, vol. 101, n. 10, October 2013 Proceedings of the IEEE, p. 2299/2305. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=06600843>. Acesso em: 15 set. 2013.

HOW to prevent mobile phone spying. SearchSecurity.com. Coluna Ask the Expert. Disponível em: <http://searchsecurity.techtarget.com/answer/How-to-prevent-mobile-phone-spying>. Acesso em 30 set. 2013.

HUURDEMAN, Anton A., **The world wide history of telecommunications**. Hoboken: John Wiley & Sons, Inc., 2003.

IEEE GLOBAL HISTORY NETWORK. Disponível me: <http://www.ieeeghn.org>. Acesso em: 01 ago. 2013.

IP-ADRESS.COM. Produced by Paul Internet. Homburg, Germany. Disponível em: <http://www.ip-adress.com/>. Acesso em: 03 set. 2013.

IRLANDA. Department of Communications, Energy and Natural Resources. Disponível em: <http://www.dcenr.gov.ie/>. Acesso em: 14 mai. 2013.

_____. Irish Statute Book. Produced by The Office of the Attorney General. Disponível em: < http://www.irishstatutebook.ie/>. Acesso em: 14 mai. 2013.

JABUR, Gilberto Haddad. **Liberdade de pensamento e direito à vida privada**: conflitos entre direitos da personalidade. São Paulo: Revista dos Tribunais, 2000.

JORDÃO, Fabio. **O que é IP estático? E dinâmico?**. 2009. Disponível em: <http://www.tecmundo.com.br/1836-o-que-e-ip-estatico-e-dinamico-.htm>. Acesso em: 02 set. 2013.

KARAM, Maria Lúcia. **Interceptação de comunicações telefônicas**: o Estado máximo, vigilante e onipresente. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/anexos/10286-10286-1-PB.html>. Acesso em: 10 mar. 2012.

KERR, Orin S. **Lifting the "fog" of internet surveillance**: How A Suppression Remedy Would Change Computer Crime Law. Public Law and Legal Theory Research Paper No. 057. The George Washington University Law School, 2003.

KUROKAWA, Adriana Shimabukuro et al. **Crimes cibernéticos**: manual prático de investigação. São Paulo: Ministério Público Federal, Procuradoria da República do Estado de São Paulo, Grupo de Combate aos Crimes Cibernéticos, 2006.

LAW, David S. **Generic Constitutional Law**. University of San Diego School of Law Public Law and Legal Theory Research Paper Series. paper 23. The Berkeley Electronic Press. 2004. Disponível em: <http://law.bepress.com/cgi/viewcontent.cgi?article=1015&context=sandiegolwps-pllt>. Acesso em: 01.05.2013.

LEWIS, Paul. You're being watched: there's one CCTV camera for every 32 people in UK, **The Guardian**. 02 mar. 2011. Disponível em: <http://www.guardian.co.uk/uk/2011/mar/02/cctv-cameras-watching-surveillance>. Acesso em: 28 jun. 2013.

LIEBMAN, Enrico Tullio. **Unità del procedimento cautelare**. Problemi del processo civile. Napoli: Morano, 1962.

LLOYD, Ian James. The Interception of Communications Act 1985. In: **The Modern Law Review**, vol. 49, n. 1, 1986, p. 88. Disponível em: <http://onlinelibrary.wiley.com/doi/10.1111/j.1468-2230.1986.tb01679.x/pdf>. Acesso em: 12 nov. 2013.

LOPES JR., Aury. **Direito processual penal e sua conformidade constitucional**. v. I. 3ª ed. Rio de Janeiro: Lumen Juris, 2008.

LÓPEZ, Juan José González. Intervención de comunicaciones: nuevos desafíos, nuevos límites. In: GIL, J. P. (Coord.). **El proceso penal en la sociedad de la información**: las nuevas tecnologías para investigar y probar el delito. Madrid: La Ley, 2012.

_____. **Los datos de tráfico de las comunicaciones electrónicas en el proceso penal**. Madrid: La Ley, 2007.

LOWENSTEIN, Karl. **Teoria de la Constitución**. Tradução Alfredo Galego Anabitarte. Barcelona, Ediciones Ariel, 1970.

MACHADO, André Augusto Mendes; KEHDI, Andre Pires de Andrade. A. **A investigação criminal defensiva**. 2009. Dissertação (Mestrado em Processo Penal) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2009.

_____; KEHDI, Andre Pires de Andrade. Sigilo das comunicações de dados. In: FERNANDES, Antonio Scarance; ALMEIDA, José Raul Gavião de; MORAES, Maurício Zanoide de. (Coord.). **Sigilo no processo penal**: eficiência e garantismo. São Paulo: Revista dos Tribunais, 2008.

MAHMOUD, Mohamad Ale Hasan. Internet protocol e autorização judicial. **Boletim do Instituto Brasileiro de Ciências Criminais**, São Paulo, n. 205, v. 17, p. 7-8, 2009.

MALAN, Diogo Rudge. **Interceptação telemática** [mensagem pessoal]. Mensagem recebida por <sidi@ffernandes.adv.br> em 12 nov. 2012.

MARQUES, José Frederico. **Elementos de direito processual penal**. v. IV. Rio de Janeiro: Forense, 1965.

_____. **Elementos de direito processual penal**. v. I. Campinas: Bookseller, 1997.

_____. **Tratado de direito processual penal**. v. I. São Paulo: Saraiva, 1980.

MAXIMILIANO, Carlos. **Hermenêutica e aplicação do direito**. 9ª ed. Rio de Janeiro: Forense, 1981.

MCCULLAGH, Declan; BROACHE, Anne. FBI taps cell phone mic as eavesdropping tool. **CNET News**. 01 dec. 2006. Disponível em: <http://news.cnet.com/2100-1029-6140191.html>. Acesso em: 25 set. 2013.

MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**. 2ª ed. rev. e atual. São Paulo: Saraiva, 2008.

MIRANDA, Jorge. **Teoria do Estado e da Constituição**. Coimbra: Coimbra Editora, 2002.

MORAES, Alexandre de. A constitucionalidade do parágrafo único do art. da Lei n. 9296/96: interceptações do fluxo de comunicações em sistemas de informática e telemática. **Boletim do Instituto Brasileiro de Ciências Criminais**, São Paulo, n. 54, p. 5, 1997.

MORI, Michele Keiko. **Direito à intimidade versus informática**. Curitiba: Juruá, 2001.

NSA leak: Source believes exposure, consequences inevitable. **The Washington Post**. 06 jun. 2013. Disponível em: <http://www.washingtonpost.com/posttv/video/thefold/nsa-leak-source-

believes-exposure-consequences-inevitable/2013/06/07/fb15c0fe-cf94-11e2-8845-d970ccb04497_video.html>. Acesso em: 15 set. 2013.

NSA slides explain the PRISM data-collection program. **The Washington Post**. 06 jun. 2013. Disponível em: <http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/>. Acesso em: 15 set. 2013.

NUCCI, Guilherme de Souza. **Código de Processo Penal comentado**. 10ª ed. São Paulo: Revista do Tribunais, 2011.

_____. **Leis penais eprocessuais penais comentadas**. 5ª ed. São Paulo: Revista dos Tribunais, 2010.

ODELL, Mark. Use of mobile helped police keep tabs on suspect and brother. **Financial Times**. 02 ago. 2005. Disponível em: <http://cdn.ca9.uscourts.gov/datastore/library/2013/02/26/Oliva_FinancialTimes.pdf>. Acesso em: 29 set. 2013.

OXFORD DICTIONARIES ONLINE. Oxford University Press. Disponível em: <http://oxforddictionaries.com>. Acesso em: 10 set. 2013.

PERALES, Ascensión Elvira. Sinopsis. Diciembre 2003, Actualizado por Ángeles González Escudero en octubre de 2006. Enero 2011. Disponível em: <http://www.congreso.es/consti/constitucion/indice/sinopsis/sinopsis.jsp?art=18&tipo=2>. Acesso em: 03 nov. 2013.

PEREIRA, Caio Mario da Silva. **Direito civil**: alguns aspectos da sua evolução. Rio de Janeiro: Forense, 2001.

PERLROTH, Nicole; LARSON, Jeff; SHANE, Scott. N.S.A. Able to Foil Basic Safeguards of Privacy on Web. **The New York Times**. 05 set. 2013. Disponível em: <http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=all&_r=0>. Acesso em 27 set. 2013.

PIAZERA, Isadora Bolduan. **RE: Esclarecimentos** [mensagem pessoal]. Mensagem recebida por <sidi@ffernandes.adv.br> em 14 out. 2013.

PITOMBO, Sergio Marcos de Moraes. Inquérito policial: exercício do direito de defesa. **Boletim do Instituto Brasileiro de Ciências Criminais**, São Paulo, nº 83. edição especial. Out/1999.

PORTUGAL. **Diário da República**, 1ª série - Nº 179 - 15 de Setembro de 2009. Disponível em: <http://dre.pt/pdfgratis/2009/09/17900.pdf>. Acesso em: 15 mar. 2012.

_____. **Diário da República.** Convenção do Conselho da Europa sobre Cibercrime, artigos 2º a 10º. Disponível em: <http://dre.pt/pdfgratis/2009/09/17900.pdf>. Acesso em: 29 jan. 2012.

PRADO, Geraldo Luiz Mascarenhas. **Limite às interceptações telefônicas e a jurisprudência do Superior Tribunal de Justiça**. 2ª ed. Rio de Janeiro: Lumen Juris, 2006.

PREMIO oferecido de US$250,000: + de 5000 Hackers & Spies Competindo: Não há vencedores: E, francamente, nós não estamos surpresos. GOLD LOCK Gold Line Group Ltd. Disponível em: <https://www.gold-lock.com/pt/hackerchallenge/>. Acesso em: 27 set. 2013.

PROPOSTAS de emendas ao Projeto de Lei de Código de Processo Penal. Substitutivo CCJ do Senado. Instituto Brasilero de Direito Processual (IBDP). Disponível em: <http://www.direitoprocessual.org.br/download.php?f=9546b22fe462eb3d2116f6ff5b62a312>. Acesso em: 05 jan. 2014.

RAMOS, João Gualberto Garcez. **Curso de processo penal norte-americano**. São Paulo: Revista dos Tribunais, 2006.

REID, S. Alan; RYDER, Nicholas. **For Whose Eyes Only?** A Critique of the United Kingdom's Regulation of Investigatory Powers Act 2000, Information & Communications Technology Law, vol. 10, Iss. 2, 2001.

REINO UNIDO. 2012 Annual Report of the Interception of Communications Commissioner: Presented to Parliament pursuant to Section 58(6) of the Regulation of Investigatory Powers Act 2000, The Stationery Office Limited, London, 2013. Disponível em: <http://www.iocco-uk.info/docs/2012%20Annual%20Report%20of%20the%20Interception%20of%20Communications%20Commissioner%20WEB.pdf>. Acesso em: 12 set. 2013

_____. **A Strong Britain in an Age of Uncertainty**: The National Security Strategy. Presented to Parliament by the Prime Minister by Command of Her Majesty. London: The Stationery Office, 2010. Disponível em: <http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf?CID=PDF&PLA=furl&CRE=nationalsecuritystrategy>. Acesso em: 18 ago. 2013.

_____. England and Wales Court of Appeal (Criminal Division). R v. S and another. 2008 EWCA Crim 2177; [2008] All ER (D) 89 (Oct). Disponível em: <http://www.lexisnexis.com/lnacui2api/api/version1/getDocCui?lni=4TMY-HYH0-01NS-Y0YD&csi=145262&hl=t&hv=t&hnsd=f&hns=t&hgn=t&oc=00240&perma=true>. Acesso em: 17 jul. 2013.

_____. Investigatory Powers Tribunal. Disponível em: <http://www.ipt-uk.com/default.asp?sectionID=16>. Acesso em: 06 jul. 2013.

_____. The National Archives on behalf of Her Majesty's Government. Her Majesty's Stationery Office (HMSO). Disponível em: <http://www.legislation.gov.uk>. Acesso em: 02 ago. 2013.

REIS, Flávia Michele Medeiros de Araújo. **RE: Esclarecimentos** [mensagem pessoal]. Mensagem recebida por <sidi@ffernandes.adv.br> em 14 out. 2013.

REIS, José Carlos Vasconcellos dos. Controle Externo do Poder Judiciário e separação de poderes. In: QUARESMA, Regina; OLIVEIRA, Maria Lúcia de Paula (Coord.). **Direito Constitucional Brasileiro**: perspectivas e controvérsias contemporâneas. Rio de Janeiro, Forense, 2006.

RODRIGUES, Benjamim Silva. **A monitorização dos fluxos informacionais e comunicacionais**. v. I. Coimbra: Coimbra Editora, 2009.

ROHR, Altieres. Entenda como funcionam os grampos de celular. **G1**. 14 abr. 2012. Disponível em: <http://g1.globo.com/platb/seguranca-digital/2012/04/14/entenda-como-funcionam-os-grampos-de-celular/>. Acesso em: 29 set. 2013.

ROWBOTTOM, Jacob H. To Rant, Vent And Converse: Protecting Low Level Digital Speech. **Cambridge Law Journal**. v. 71. Paper No 17/2012. 02 abr. 2012. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2033106>. Acesso em: 07 mar. 2013.

SCHIER, Paulo Ricardo. As comissões parlamentares de inquérito e a defesa dos direitos individuais. In: **Revista da Acacemia Brasileira de Direito Constitucional**: anais do IV Simpósio Brasileiro de Direito Constitucional, v. 3. Curitiba: ABDC, 2003.

SILVA JR., José. **Telemática** [mensagem pessoal]. Mensagem recebida por <sidi@ffernandes.adv.br> em 09 out. 2013.

SILVA, Edson Ferreira da. **Direito à intimidade**: de acordo com a doutrina, o direito comparado, a Constituição de 1988 e o Código Civil de 2002. 2ª ed. São Paulo: J. de Oliveira, 2003.

SILVA, José Afonso da. **Curso de direito constitucional positivo**. São Paulo: Malheiros, 2010.

SILVA, Ovídio A. Batista da. **As ações cautelares e o novo processo civil**. 3ª ed. Rio de Janeiro: Forense, 1980.

SILVA, Virgílio Afonso da. **Direitos fundamentais**: conteúdo essencial, restrições e eficácia. 2ª ed. São Paulo: Malheiros, 2010.

SINGEL, Ryan. Point, Click ... Eavesdrop: How the FBI Wiretap Net Operates. **Wired Magazine.** 29 ago. 2007. Disponível em: <http://www.wired.com/politics/security/news/2007/08/wiretap?currentPage=all>. Acesso em: 02 fev. 2013.

SIQUEIRA JÚNIOR, Paulo Hamilton. **Comissão Parlamentar de Inquérito**. Rio de Janeiro, Elsevier, 2007.

STAHL, Bernd Carsten. The impact of the UK Human Rights Act 1998 on privacy protection in the workplace. RAMESH, Subramanian (Org.). **Computer Security, Privacy and Politics**: current issues, challenges, and solutions. Hershey: IGI Global, 2008, p. 55/68.

STEVENS, Gina Marie; DOYLE, Charles. **Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping**. Congressional Research Service, CRS Report for Congress. Prepared for Members and Committees of Congress, October 9, 2012.

STRECK, Lenio Luiz. **As interceptações telefônicas e os direitos fundamentais**. 2ª ed. Porto Alegre: Livraria do Advogado, 2001.

SUNTECH GRUPO VERINT. Disponível em: <http://www.suntechintelligence.com/>. Acesso em: 26 ago. 2013.

SUNTECH VIGIA. Interception Achievement Suite. Manual do Usuário Vigia 3. Outubro/2011. Disponível em: <https://vigia.claro.com.br/VigiaDadosClient/custom/doc/Manual_VIGIA3_Consulta.pdf;jsessionid=17AC1571FB9CF8BA129C7D3821809BC9.tomcat1>. Acesso em: 14 out. 2013.

TELECO INTELIGÊNCIA EM TELECOMUNICAÇÕES. Disponível em: <http://www.teleco.com.br>. Acesso em: 01 out. 2013.

TICAMI, Danilo Dias; ALBUQUERQUE, Poliana Soares. Minority Report: a nova lei e velhos devaneios repressivistas. In: **Revista Liberdades**, São Paulo, nº 11 - setembro/dezembro de 2012, Publicação Oficial do Instituto Brasileiro de Ciências Criminais.

TONINI, Paolo. **A prova no processo penal italiano**. Tradução Alexandra Martins e Daniela Mróz. São Paulo: Revista dos Tribunais, 2002.

_____. **La prova penale**. 4ª ed. Padova: Cedam, 2000.

TOURINHO FILHO, Fernando da Costa. **Manual de processo penal**. 8ª ed. São Paulo: Saraiva, 2006.

_____, Fernando da Costa. **Processo penal**. v. 3. 21ª ed. São Paulo: Saraiva, 1999.

TRIBUNAL EUROPEU DE DIREITOS HUMANOS. Caso Campbell vs. The United Kingdom. Disponível em: <http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=campbell&sessionid=90267778&skin=hudoc-en>. Acesso em: 01 abr. 2012.

_____. Caso Dudgeon vs. The United Kingdom. Disponível em: <http://cmiskp.echr.coe.int/tkp197/view.asp?item=2&portal=hbkm&action=html&highlight=dudgeon&sessionid=90267778&skin=hudoc-en>. Acesso em: 01 abr. 2012.

_____. Caso Funke vs. France. Disponível em: <http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=funke&sessionid=90267778&skin=hudoc-en>. Acesso em: 03 abr. 2012.

_____. Caso Gillow vs. The United Kingdom. Disponível em: <http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=gillow&sessionid=90267778&skin=hudoc-en>. Acesso em: 03 abr. 2012.

_____. Caso Klass et al. vs. Germany. Disponível em: <http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=klass&sessionid=90267778&skin=hudoc-en>. Acesso em: 07 abr. 2012.

_____. Caso Kopp vs. Suíça. Disponível em: <http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=kopp&sessionid=90267778&skin=hudoc-en>. Acesso em: 01 abr. 2012.

_____. Caso Malone vs. The United Kingdom. Disponível em: < http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-57533>. Acesso em 07 mai. 2013.

_____. Caso Olsson vs. Sweden. Disponível em: <http://cmiskp.echr.coe.int/tkp197/view.asp?item=2&portal=hbkm&action=html&highlight=olsson&sessionid=90267778&skin=hudoc-en>. Acesso em: 07 abr. 2012.

TUCCI, Rogério Lauria. **Direitos e garantia individuais no processo penal brasileiro**. 3ª ed. rev. atual. e ampl. São Paulo: Revista dos Tribunais, 2009, p. 75.

TUTORIALSPOINT. Disponível em: <http://www.tutorialspoint.com/>. Acesso em: 30 ago. 2013.

UBERTIS, Giulio. **La prova penale**: profili giuridici ed epistemologici. Torino: Utet, 1999.

UICICH, Rodolfo Daniel. **El derecho a la intimidad en internet y en las comunicaciones electrónicas**. Buenos Aires: Ad-Hoc, 2009.

VIEIRA DE ANDRADE, José Carlos. **Os direitos fundamentais na Constituição Portuguesa de 1976**. 5ª ed., Coimbra, Almedina, 2012.

WARREN, Samuel Dennis; BRANDEIS, Louis Dembitz. The right to privacy. **Harvard Law Review**, v. IV, nº 5, 15.12.1890, Disponível em: <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>. Acesso em: 05 mai. 2012.

WHEELER, Brian. This goes no further... **BBC News Online Magazine**. 02 mar. 2004. Disponível em: <http://news.bbc.co.uk/2/hi/uk_news/magazine/3522137.stm>. Acesso em: 29 set. 2013.

WIRELESS DICTIONARY. Disponível em: <http://www.wirelessdictionary.com/>. Acesso em: 05 set. 2013.

WU, Dapeng. **Streaming video over the internet**: approaches and directions. IEEExplore

digital Library. mar. 2011. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=911156>. Acesso em: 05 abr. 2013.

YOUNKER, Emily. **How Digital Radio Works**. Disponível em: <http://digital-radio-review.toptenreviews.com/how-digital-radio-works.html>. Acesso em: 25 ago. 2013.

ZILLI, Marcos Alexandre Coelho. **A iniciativa instrutória do juiz no processo penal**. São Paulo: Revista dos Tribunais, 2003.