ano 2 - n. 4 | julho/dezembro - 2015
Belo Horizonte | p. 1-320 | ISSN 2319-0795
R. Fórum de Ci. Crim. – RFCC

Revista Fórum de CIÊNCIAS CRIMINAIS

RFCC

EDITORA Fórum

REVISTA FÓRUM DE CIÊNCIAS CRIMINAIS – RFCC

Luís Cláudio Rodrigues Ferreira
Presidente e Editor

Av. Afonso Pena, 2770 – 16º andar – Funcionários – CEP 30130-007 – Belo Horizonte/MG – Brasil – Tel.: 0800 704 3737
www.editoraforum.com.br / E-mail: editoraforum@editoraforum.com.br

Impressa no Brasil / Printed in Brazil / Distribuída em todo o Território Nacional

R454 Revista Fórum de Ciências Criminais – RFCC. –
ano 1, n. 1, (jan./jun. 2014)- . – Belo Horizonte:
Fórum, 2014-

Semestral
ISSN 2319-0795
1. Direito penal. 2. Ciência criminal. I. Fórum.

CDD: 341.5
CDU: 343

Esta revista está catalogada em:
• RVBI (Rede Virtual de Bibliotecas – Congresso Nacional)

Supervisão editorial: Leonardo Eustáquio Siqueira Araújo
Capa: Igor Jamur
Projeto gráfico: Walter Santos
Ilustração: Isabela Palmer

A interceptação de *e-mails* e a apreensão física de *e-mails* armazenados[1]

Ricardo Sidi

Advogado. Mestre em Processo Penal pela Universidade de São Paulo (USP). Pós-graduado em Direito Penal Empresarial pela PUC-Rio. Pós-graduado em Criminologia, Direito e Processo Penal pela Universidade Cândido Mendes (UCAM). Professor do Curso de Pós-Graduação de Direito Processual e os Reflexos da Tecnologia da Informação da Universidade de São Paulo (USP).

Resumo: O artigo analisa o sigilo sobre a comunicação via *e-mail*, sobre mensagens armazenadas em discos rígidos do suspeito ou de seu provedor e sobre os dados de tráfego de comunicações (também chamados de dados externos ou não humanos), verificando, à luz do princípio da proporcionalidade, dos padrões concebidos pelas cortes regionais de direitos humanos e de um parâmetro doutrinário de eficiência e garantismo do processo penal, se esse sigilo está inserido ou excluído do âmbito de proteção do direito constitucional ao sigilo das comunicações (art. 5º, XII, da Constituição Federal).

Palavras-chave: Direito ao sigilo das comunicações. Interceptação de *e-mails*. Apreensão de *e-mails* armazenados. Dados de tráfego de comunicações.

1 Interceptação

A medida de interceptação de comunicações é uma providência cautelar[2] que constitui um meio de obtenção de prova,[3] [4] que terá como resultado uma fonte de prova[5] que será inserida no processo através de uma mídia (como DVD ou *pendrive*), que, por sua vez, constituirá um meio de prova documental.[6]

1 Artigo escrito a convite do Conselho Editorial.

2 FERNANDES. 2010, p. 96.

3 Luiz Flavio Gomes e Raúl Cervini (1997, p. 116) 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)". Grinover, Gomes Filho e Scarance Fernandes (2009, p. 165) 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".

4 Segundo a classificação adotada por Aury Lopes Jr. (2008, p. 500), a medida de interceptação telemática é um ato de investigação.

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

6 GRINOVER; GOMES FILHO; FERNANDES, *loc. cit.*: "Meio de prova será o documento (a gravação e sua transcrição) a ser introduzido no processo". Para Lopes Jr. (2008, p. 636-637), o conceito de documento incluiria

Há um consenso, inclusive noutros ordenamentos, em se definir a expressão "interceptação" como uma operação de captação de uma comunicação contemporânea, no momento em que esteja ocorrendo.

Para o espanhol Juan López (2012), "*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*".[7]

No caso *United States v. Jones*, a *United States District Court for the District of Columbia* afirmou que o regime legal 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 repousam em arquivo eletrônico mantido por terceiros.[8]

Também a *United States Court of Appeals for the Eleventh Circuit*, no caso *United States v. Steiger*, afirmou que a aquisição de dois *e-mails* extraídos remotamente do disco rígido do investigado não se enquadrava no conceito de interceptação, pois não fora contemporânea, ou seja, não se deu no momento da transmissão, mas, sim, quando eles já repousavam num computador.[9]

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). 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 (2000, p. 190): "*Ebbene, i documenti si qualificano appunto come prove precostituite e, pertanto, si pongono come eccezioni alia regola dell'immediatezza*".

7 LÓPEZ. 2012, p. 119.

8 *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.').* (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).

9 *"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).* (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).

2 Inviolabilidade, absoluta ou não, do sigilo da comunicação por *e-mail*

No Brasil, diante da ambígua redação do inciso XII do artigo 5º da Constituição Federal,[10] várias são as divergências em torno da interpretação do dispositivo.

Para Tércio Sampaio Ferraz (1993), a Constituição assegura o sigilo de dados relativamente à comunicação no interesse da defesa da privacidade,[11] 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.[12] O autor observa que, dos quatro meios de comunicação ali mencionados, ou seja, correspondência, telegrafia, dados e telefonia, só o último se caracterizaria por sua instantaneidade, ou seja, é o único que não deixa vestígios, sendo a interceptação sub-reptícia a única forma de se preservar o conteúdo da comunicação.[13]

No que se refere, por exemplo, à movimentação bancária de um indivíduo, Tércio Ferraz, em coerência com 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.[14]

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,[15] pois diversas são as formas de comunicação de dados que não geram o armazenamento do teor do diálogo.[16]

Geraldo Prado (2006) posiciona-se 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.[17]

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 deveria ser o meio de comunicação utilizado, mas, sim, o processo comunicante,[18] a partir do qual se poderia constatar se o teor das comunicações se

[10] Art. 5º (...) XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;

[11] Segundo o autor, intimidade se liga a aspectos não compartilhados com absolutamente ninguém.

[12] FERRAZ JR. 1993, p. 446.

[13] *Ibid.*, p. 447-448.

[14] *Ibid.*, p. 452.

[15] BADARÓ. 2010, p. 490.

[16] Pode-se citar o Skype e o MSN quando utilizados na modalidade de voz (não escrita), o FaceTime e o VoIP.

[17] PRADO. 2006, p. 73.

[18] BADARÓ. 2010, p. 491 (nota de rodapé 26).

pereniza de alguma forma e se, assim, é ou não passível de apreensão. É diante disso que Badaró afirmou que *e-mail* (que se pereniza) se sujeita a uma inviolabilidade absoluta,[19] 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.[20]

Chegamos, no entanto, à conclusão diversa daquela adotada pelos autores acima.

Realmente, vedar a interceptação de *e-mail* em razão da possibilidade de apreensão física posterior das mensagens atende o princípio da proporcionalidade em seu subprincípio[21] ou máxima parcial[22] da necessidade, segundo o qual a medida adotada deve ser a menos gravosa e onerosa possível para o cidadão. Porém, a nosso ver, tornar a comunicação via *e-mail* arrecadável exclusivamente por meio de apreensão física retiraria dos órgãos de persecução uma celeridade que lhes seria elementar para a eficiência do exercício de seu múnus, desatendendo, assim, o subprincípio da adequação, segundo o qual a medida adotada para realizar o interesse público deve ser apropriada à obtenção do fim pretendido.[23]

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) esteja *online*, acessível em tempo real através de algum meio comunicativo moderno.

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 art. 225, §3º, todos da CF) sejam providos de condições para atuar nesses novos tempos de forma equilibrada segundo um critério de eficiência e garantismo.[24]

[19] *Ibid.*, p. 492.
[20] *Ibid.*, p. 493.
[21] CANOTILHO. 2000, p. 269-270.
[22] ALEXY. 2011, p. 116-117.
[23] CANOTILHO. *loc. cit.*
[24] O binômio eficiência e garantismo traz concepções que foram pontuadas por Antonio Scarance Fernandes em três célebres publicações. A primeira concepção é a de que tanto o direito à segurança quanto à liberdade constituem interesses relevantes (no Brasil, ambos estão inseridos no *caput* do art. 5º da CF), 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. 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. A segunda concepção é a de que deve haver um equilíbrio adequado, no meio do caminho entre o que o Professor Scarance Fernandes 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.

Observa-se que a realidade histórica das tecnologias comunicativas que inspiraram a 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.

A nosso ver, o só fato de a hoje tão popular e célere comunicação por *e-mail* poder ser alvo de apreensão física posterior, num disco rígido do investigado ou de seu provedor, não é o bastante para impedir que o Estado lance mão da captação contemporânea por meio de interceptação, sob pena de fazer a balança pender excessivamente para o lado do hipergarantismo e afastar o ordenamento do ponto médio pretendido entre eficiência e garantismo.

3 Dados de tráfego e sua inserção no âmbito de proteção do direito ao sigilo das comunicações

Na comunicação entre dois indivíduos, sendo um o emissor da mensagem, e outro, o 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 da 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[25] 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.

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. 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. 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. (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). Ada Pellegrini Grinover (1996, p. 278) 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. No entanto, também não vê incompatibilidade entre garantismo e eficiência, que diz constituírem os valores fundamentais do novo processo latino-americano.

[25] Estações rádio base (ERBs) vêm a ser as antenas ou torres de telefonia móvel.

A legislação britânica definiu os dados de tráfego como aqueles que identifiquem as pessoas, os aparelhos ou a localização de onde ou para onde a comunicação esteja sendo transmitida.[26]

A Diretiva 2002/58 da Comunidade Europeia os definiu 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).[27]

A lei espanhola, por sua vez, definiu os dados de tráfego como aqueles capazes de identificar os interlocutores, seus 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.[28]

---

[26] *Regulation of Investigatory Powers Act 2000* (RIPA). "*2 Meaning and location of "interception" etc. (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).

[27] Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32002L0058>. Acesso em: 31 jul. 2015.

[28] Ley 25/2007. "*Artículo 1. Objeto de la Ley. (...) 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. 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. 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.º 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.º 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.º 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*

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 nº 9.296/96, não abarcam o sigilo de dados que repousem em servidores, *hard disks* e sistemas de instituições bancárias, mas apenas a comunicação envolvendo esses dados.[29]

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[30] geral da intimidade e da vida privada (art. 5º, X, CF),[31] inclusive no que se refere aos dados armazenados relativos às próprias ligações telefônicas, ou seja, os registros de horários de chamadas, sua duração, números de origem e do destinatário não seriam protegidos pela inviolabilidade do sigilo das comunicações, mas, sim, pelo inciso X do artigo 5º da CF.[32]

Também noutros ordenamentos, verifica-se essa mesma tendência.

Na legislação britânica, 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 *Regulation of Investigatory Powers Act 2000* (RIPA), na qual tais dados

---

su caso, del servicio de mensajería o del servicio multimedia. 2.º 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.º 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.º 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.º 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.º 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.º La etiqueta de localización (identificador de celda) al inicio de la comunicación. 2.º 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 maio 2013).

[29] 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). (MENDES; COELHO. 2008, p. 392).

[30] Ressalvamos que concluímos se tratar de um direito geral à intimidade (SIDI. 2014, p. 19).

[31] BADARÓ. 2010, p. 485.

[32] 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 radio base) das companhias de telefonia celular.

são tratados por *communication data*.[33] 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 a fim de detectar ou prevenir um crime ou a desordem, preservar o bem-estar econômico do Reino Unido, preservar a segurança pública e a saúde pública, 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, 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.[34]

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

Nos Estados Unidos, 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 o Congresso destinou menor proteção aos conteúdos armazenados do que àqueles que estejam em seu momento de transmissão.[35]

---

[33] 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).

[34] 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).

[35] 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. *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*

Na Espanha, verifica-se um critério temporal reconhecido, no Recurso de Amparo 3787-2001, pelo *Tribunal Constitucional*, 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 das comunicações, mas pela norma protetora da intimidade, do artigo 18.1 da Constituição espanhola.[36]

Mas, no Recurso de Casación 121/2009, o *Tribunal Supremo* espanhol adotou método bastante lúcido de distinção entre dados atinentes e não atinentes ao sigilo das comunicações. A Corte distinguiu dados que possam afetar o sigilo das comunicações daqueles que, embora conservados por operadoras de comunicações, sejam estaticamente armazenados, mas que não se refiram à comunicação alguma, concebendo 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

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 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).

[36] *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.* (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).

estes protegidos pelo direito à proteção de dados informáticos ou *habeas data* assegurados no artigo 18.4 da Constituição.

Concluiu, a partir dessa perspectiva dicotômica, que os dados relativos a comunicações concretamente realizadas são os que estão compreendidos no âmbito de proteção do artigo 18.3, pois a inclusão absoluta de todo tipo de dado de tráfego ou externo sob a mesma proteção acabaria por igualar circunstâncias cujo tratamento jurídico deveria ser distinto.[37]

A nosso ver, os termos com os quais o constituinte brasileiro concebeu a inviolabilidade do "sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas" não deixa dúvida de que a proteção dada ao conteúdo humano do que um interlocutor fala ou escreve para o outro se estende aos detalhes que estejam ligados a uma comunicação real, concreta, que tenha efetivamente existido. Raciocinar o contrário seria sustentar que não integram o sigilo de uma comunicação a identidade do interlocutor, a duração da conversa e a localização geográfica dos indivíduos envolvidos no momento em que ocorria determinada comunicação, com o que não podemos concordar.

---

[37] *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 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.* (ESPANHA. Tribunal Supremo. Sala de lo Penal. STS 1550/2010. Recurso de 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).

Não é razoável, por exemplo, se revelar, a partir de dados armazenados numa operadora, que Tício, em todas as madrugadas, se comunica com Cássia por duas horas, enquanto esta se encontra posicionada na casa de seu namorado, e pretender que tal revelação não diga respeito ao sigilo das comunicações desses indivíduos.

Portanto, concluímos, da mesma forma que o precedente espanhol, que determinados dados de tráfego ou externos se inserem no âmbito de proteção do direito ao sigilo das comunicações, precisamente aqueles ligados a comunicações concretas, enquanto aqueles desconectados de comunicações concretas estarão protegidos, meramente, pelo direito geral à intimidade.

Exemplos de dados que fogem à esfera de proteção do direito à inviolabilidade do sigilo das comunicações serão, portanto, os dados identificadores de aparelhos (a exemplo do código IMEI)[38] e do usuário (a exemplo do IMSI);[39] e o IP do assinante pesquisado (quando for fixo ou estático),[40] mas jamais do interlocutor que possa ter se comunicado com o alvo, já que tal informação dependeria do acesso a detalhes de uma comunicação concreta, além dos dados cadastrais de assinantes.

Já exemplos de dados indissociáveis de comunicações concretamente ocorridas e que estarão preservados sob o manto da proteção ao sigilo das comunicações serão o IP (dinâmico), utilizado numa 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.

A relevância prática da distinção é que, enquanto o acesso estatal aos dados comunicativos protegidos pelo direito geral à intimidade (art. 5º, X, CF) deverá obedecer aos artigos 240 e seguintes do CPP, o acesso àqueles protegidos pelo direito ao sigilo das comunicações (art. 5º, XII, CF) deverá seguir a Lei nº 9.296/96, claramente mais rigorosa.

4 *E-mails* armazenados

Observe-se que tudo que aqui se expôs em relação à inserção dos dados de tráfego vinculados a comunicações concretas no âmbito de proteção do direito ao

[38] 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).

[39] 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).

[40] Isto porque o IP variável ou dinâmico, para ser revelado, precisará estar vinculado a uma comunicação concreta.

sigilo das comunicações terá que ser, obviamente, aplicável, e com muito maior razão, a mensagens de e-mail armazenadas em servidores de provedores e em discos rígidos pertencentes a investigados, pois nelas estará o próprio conteúdo humano das comunicações.

Retirar conteúdos humanos de comunicações concretamente ocorridas do âmbito normativo do direito ao sigilo das comunicações não sobreviveria ao teste do critério da especificidade de Friedrich Müller, porquanto constituem elementos típicos[41] e estruturalmente necessários[42] de seu exercício. Também não poderia a proteção a esses conteúdos ser classificada como uma circunstância meramente acidental do exercício do direito.[43]

Não há coerência ou razoabilidade em retirar os *e-mails* armazenados do âmbito de proteção do direito ao sigilo de comunicações (art. 5º, XII, CF). Afinal, por mais que sua arrecadação já não caracterize uma interceptação propriamente dita, por falta do requisito contemporaneidade, e por mais que se trate de mensagem já recebida pelo destinatário, é inegável que a preservação de seu conteúdo humano e demais detalhes ligados a ela não podem ser dissociados da expressão constitucional "sigilo das comunicações", dotada de tão claro sentido linguístico.

Veja-se que, dos ordenamentos acima analisados, o britânico e o americano não são dotados de nenhum dispositivo de hierarquia constitucional que, com a clareza do brasileiro, assegure ao indivíduo um direito ao sigilo das comunicações. No Reino Unido, sequer existe uma constituição escrita, mas, sim, um conjunto de *acts*, *statutes*, *settlements* e textos como a *Magna Cartha* (1215) e a *Bill of Rights* (1689),[44] que nada dispõem sobre comunicações.

As Convenções Europeia e Americana de Direitos Humanos, um pouco mais próximas da proteção constitucional brasileira, protegem o direito à vida privada, ao domicílio e à correspondência (artigos 8 e 11, respectivamente).

Nos Estados Unidos, a Quarta Emenda à Constituição, base da proteção às comunicações dos indivíduos, limita-se a trazer dispositivo genérico sobre um direito contra buscas e apreensões arbitrárias nas casas das pessoas.[45]

---

[41] Num primeiro exemplo célebre, Müller (1990, p. 64, 73, 74, 88, 93 e 98) 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. Num segundo exemplo, também clássico, Müller (1969, p. 59) 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. (*apud* SILVA. 2010, p. 88).

[42] SILVA. 2010, p. 88.

[43] MENDES; COELHO; BRANCO. 2008, p. 290.

[44] LAW. 2004.

[45] *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*

Já o inciso XII do artigo 5º da Constituição brasileira traz uma proteção clara ao sigilo das comunicações – e, diga-se, sem nada dispor sobre interceptação ou contemporaneidade. Institui, ao mesmo tempo, uma cláusula de exceção no caso de haver ordem judicial e desde que o afastamento desse sigilo se dê "nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal".

Alguns dirão que a falta do requisito contemporaneidade retiraria dos *e-mails* armazenados sua própria condição de comunicação, com o que não podemos concordar. Parece-nos muito óbvio que o teor de uma mensagem de *e-mail* constitui por excelência uma comunicação, ainda que já esteja recebida e guardada na caixa de entrada do destinatário e na de itens enviados do remetente.

Aliás, do ponto de vista tecnológico, no que se refere à interceptação de *e-mails*, sequer seria possível distinguir-se entre mensagens em trânsito e mensagens armazenadas, pois a captação delas sempre se dará a partir de algo armazenado, conforme bem observou a *United States Court of Appeals for the Ninth Circuit*, no caso *Konop v. Hawaiian Airlines, Inc*. O acórdão registrou que o termo "interceptar" deveria ser aplicável a comunicações eletrônicas armazenadas, porque o armazenamento é um estágio obrigatório da transmissão de *e-mails*, pois eles são armazenados em diversos computadores entre o momento em que o remetente digita a mensagem e o destinatário a lê.[46]

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*. 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, pois, na internet, ao se pressionar a tecla "enviar", a mensagem passa por diversos servidores, provedores e outros computadores, divulgando-a para cada um deles com instruções

or things to be seized (Disponível em: <http://www.law.cornell.edu/constitution/fourth_amendment>. Acesso em: 13 fev. 2013).

[46] 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. *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.*

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.

Tal método, dependente de perenizações obrigatórias no meio do caminho entre remetente e destinatário, é, portanto, inerente à modernização do processo comunicativo, o que não basta para ensejar tratamento constitucional diverso, pelo que concluímos que o *e-mail* é passível de interceptação (ainda que se deseje usar nomenclatura distinta em razão da falta de contemporaneidade).

Mas resta uma questão tormentosa a ser analisada, qual seja, a dos *e-mails* já recebidos, lidos ou não, que continuem armazenados, seja por uma opção do usuário da conta (em razão de uma conduta omissiva ou comissiva de sua parte), seja por uma razão tecnológica, inerente aos modernos sistemas de *e-mail*, que se passa a analisar.

A grande maioria dos serviços de *e-mail* da atualidade operam com a tecnologia *imap* (*internet message access protocol*), diferente da antiga *pop3* (*post office protocol 3*), hoje com cada vez menos uso.

No sistema *pop3*, os provedores recebem as mensagens destinadas a seus clientes e as armazenam até o momento em que estes conectam seus computadores ao provedor, quando essas mensagens serão transferidas a eles e apagadas do provedor.[47] Já com a tecnologia *imap*, tornou-se prática mundial que os usuários mantenham nos provedores a íntegra de suas mensagens (as recebidas, as enviadas e até as que ainda estejam em fase de rascunho) para acessá-los de qualquer lugar e por meio de qualquer dispositivo (computador de casa, computador do trabalho, *smartphones*, *tablets*, etc.). Gigantes como, por exemplo, Hotmail, Yahoo e Gmail operam com a tecnologia *imap*.

Eventual ordem de monitoramento de uma conta de *e-mail*, seja *imap*, seja *pop3*, será dirigida ao provedor para que ele crie uma chamada *conta espelho*, que deverá armazenar tudo que passar pela conta do investigado-alvo dentro do período compreendido pela autorização judicial, franqueando-se ao órgão investigador acesso a essa *conta espelho*.

Ocorre que, no caso de *e-mail imap*, há notícia de juízes determinando, além da usual criação da *conta espelho*, também que o provedor permita ao órgão persecutor acessar a integralidade das mensagens armazenadas.[48] [49]

---

[47] Apesar de haver a possibilidade de se configurar o *software* gerenciador de *e-mails* (como o Microsoft Outlook) para, na modalidade *pop3*, não apagar as mensagens do servidor do provedor, tal prática nunca foi usual devido a limites de velocidade e espaço.

[48] Expeça-se ofício à Microsoft do Brasil, com ordem extensiva às suas controladoras no exterior, solicitando a criação de conta espelho, *com acesso a todas as pastas, inclusive de mensagens armazenadas*, sem conhecimento dos usuários do serviço, pela autoridade policial. Consigne-se solicitação para que *seja franqueado também o acesso às mensagens armazenadas* na caixa postal dos endereços eletrônicos, bem como aos IPs de acesso. (Decisão em pedido de quebra de sigilo telefônico nº 5049597-93.2013.404.7000/PR, 26.11.2013, 13ª VF de Curitiba, p. 50 dos autos eletrônicos).

[49] Foram juntados no procedimento: laudo pericial de extração dos arquivos disponibilizados pela Microsoft *com as mensagens arquivadas na caixa de correio eletrônico das contas* [*omissis*]@hotmail.com e [*omissis*]@hotmail.

No entanto, diferentemente do que costuma ocorrer com as contas de *e-mail pop3*, a praxe é que nas *imap* esteja a totalidade das mensagens de toda a vida do suspeito, o que, via de regra, incluirá anos ou décadas de comunicações guardadas.

Tal nível de invasão nas comunicações do indivíduo é claramente violador do princípio da proporcionalidade, mais precisamente em seus subprincípios da necessidade ou exigibilidade e proporcionalidade em sentido estrito. Segundo o primeiro, a medida estatal deverá ser o menos gravosa e onerosa possível para o cidadão, havendo que se atender, ainda, a chamada exigibilidade temporal, que pressupõe uma rigorosa delimitação no tempo de duração da medida coativa,[50] sendo certo que uma devassa nas comunicações que alguém conserva armazenadas ao longo de décadas violará esses parâmetros.

Também o subprincípio da proporcionalidade em sentido estrito[51] restará violado, pois, segundo ele, deve haver um equilíbrio entre o significado da intervenção para o atingido e os objetivos perseguidos pelo legislador.[52] Nas palavras de Canotilho (2000), devem-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.[53]

Mais do que isso, uma rápida leitura da Lei nº 9.296/96 não deixa dúvida de que o diploma foi concebido para algo dinâmico, para a captação de comunicações contemporâneas, nada dispondo sobre o acesso das agências repressoras a mensagens armazenadas.

Com tal constatação, não sustentamos que a interceptação de *e-mails* (que, pelas razões tecnológicas acima expostas, nunca serão verdadeiramente contemporâneos) seja vedada, mas, sim, que a coleta de mensagens pretéritas armazenadas pelo indivíduo ou por seu provedor não será válida se não datarem do período compreendido pela autorização judicial, que deverá ser concedida nos termos do artigo 5º da Lei nº 9.296/96.

Não tendo a Lei nº 9.296/96 estabelecido um limite temporal para o acesso do Estado a comunicações pretéritas – pois o art. 5º, bem como todo o restante do texto legal, foi concebido para interceptação de comunicações contemporâneas – a novidade tecnológica trazida pelos *e-mails imap* não pode permitir a violação do sigilo de milhares de mensagens que um indivíduo tenha armazenado ao longo de anos ou décadas de sua vida.

---

com (evento 103) e seus respectivos autos de análise (evento 104), bem como os autos circunstanciados de cada uma das contas de *e-mail* (eventos 105 a 108). (Representação de autoridade policial pela prorrogação de monitoramento nos autos 5049597-93.2013.404.7000/PR, 24.02.2014, 13ª VF de Curitiba, p. 768 dos autos eletrônicos).

50 CANOTILHO. 2000, p. 270.

51 Alexy (2011, p. 116-117) refere-se ao princípio da proporcionalidade em sentido estrito como o mandamento do sopesamento propriamente dito.

52 MENDES; COELHO; BRANCO. 2008, p. 332.

53 CANOTILHO. 2000, p. 270.

Do contrário, a medida, além de infringir os subprincípios da proporcionalidade em sentido estrito e exigibilidade temporal, também violará a exigência constitucional de que o afastamento do sigilo das comunicações se dê somente "nas hipóteses e na forma que a lei estabelecer" (art. 5º, XII).

Há que se recordar que a implementação de interceptação de comunicações antes de existir a Lei nº 9.296/96 foi considerada ilícita pelo Supremo Tribunal Federal, sob o entendimento de que "enquanto não vie[sse] a lei a estabelecer as hipóteses e a forma em que as interceptações poderão ser permitidas, não haver[ia], por enquanto, como ordená-las, pois o Código de Telecomunicações nada especifica[ria], não suprindo a ausência de lei específica". Entendimento contrário – acrescentou o Supremo – "esvaziaria por completo a garantia constitucional, na medida em que a faria vulnerável a toda forma de arbítrio judicial".[54]

Ademais, tanto a interpretação dada ao artigo 11 da Convenção Americana de Direitos Humanos[55] pela Corte Interamericana de Direitos Humanos quanto a que o Tribunal Europeu de Direitos Humanos deu ao artigo 8º da Convenção Europeia[56] são no sentido de exigir que medidas de interceptação das comunicações estejam, não só previstas em lei, mas que a lei interna indique, com 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.

No caso *Atala Riffo y Niñas v. Chile*, a Corte Interamericana afirmou que as medidas estatais invasivas deveriam estar previstas em lei e com obediência aos requisitos da adequação, necessidade e proporcionalidade.[57] Também o Tribunal Europeu reconheceu violação à Convenção Europeia no caso *Calogero Diana v. Itália*, porque a lei interna teria deixado às autoridades uma margem excessiva de discricionariedade,[58]

[54] Por todos, o *leading case* 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.

[55] CADH (Promulgada no Brasil através do Decreto nº 678/92): "Artigo 11(2) 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".

[56] 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".

[57] *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.* (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: 31 jul. 2015).

[58] *32. The Court reiterates that while a law which confers a discretion must indicate the scope of that discretion, it is impossible to attain absolute certainty in the framing of the law, and the likely outcome of any search for certainty would be excessive rigidity (see, among many other authorities, the Silver and Others judgment*

bem como no caso *Kopp v. Suíça*, porque a lei suíça não indicava com clareza as condições e a forma pelas quais as autoridades internas deveriam exercer sua discricionariedade sobre o afastamento do sigilo de comunicações.[59]

No Brasil, o direito à inviolabilidade do sigilo das comunicações contém cláusula de exceção com 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.[60]

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

previously cited, p. 33, para. 88). In this instance, however, Law no. 354 leaves the authorities too much latitude. In particular, it goes no further than identifying the category of persons whose correspondence may be censored and the competent court, without saying anything about the length of the measure or the reasons that may warrant it. The gaps in section 18 of the Law weigh in favour of rejecting the Government's argument. 33. In sum, the Italian Law does not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities, so that Mr Diana did not enjoy the minimum degree of protection to which citizens are entitled under the rule of law in a democratic society (see the Kruslin judgment previously cited, pp. 24 and 25, para. 36). There has therefore been a breach of Article 8 (art. 8). (TRIBUNAL EUROPEU DE DIREITOS HUMANOS. *Caso Calogero Diana vs. Itália*. Disponível em: <http://hudoc.echr.coe.int/eng?i=001-58072>. Acesso em: 01 ago. 2015).

[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://hudoc.echr.coe.int/eng?i=001-58144>. Acesso em: 01 ago. 2015).

[60] 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). 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).

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,[61] como fez ao impor ao legislador infraconstitucional que o afastamento do sigilo comunicativo somente poderia se dar "para fins de investigação criminal ou instrução processual penal".

5 Conclusões

Chegamos, portanto, às seguintes conclusões:

1 – O sigilo sobre os conteúdos humanos de mensagens de *e-mail*, armazenadas ou não (e demonstramos que sempre se trata de algo com estágios obrigatórios de armazenamento), está incluído no âmbito de proteção do direito ao sigilo das comunicações (art. 5º, XII, CF).

2 – Os dados de tráfego, de igual forma, estarão inseridos no âmbito de proteção do direito ao sigilo das comunicações (art. 5º, XII, CF) sempre que estiverem vinculados a comunicações concretas, mesmo método adotado pelo *Tribunal Supremo* da Espanha no Recurso de Casación 121/2009.

3 – O acesso das agências estatais a contas de *e-mail* do tipo *imap* não pode, além de contar com a usual criação das *contas espelho*, destinadas a captar mensagens trocadas pelo alvo no período contemplado pela autorização judicial, incluir o acesso a todo o teor de mensagens pretéritas armazenadas, sob pena de violação ao princípio da proporcionalidade em seus subprincípios da exigibilidade temporal e proporcionalidade em sentido estrito.

4 – O acesso estatal irrestrito a mensagens pretéritas do indivíduo importará, também, em violação aos padrões instituídos nas cortes regionais de direitos humanos em razão da falta de previsão legal da medida invasiva.

5 – Mensagens de *e-mail* arrecadadas por órgãos de persecução por meio de apreensão física de discos rígidos do suspeito ou de seu provedor constituirão elementos fortuitamente encontrados de uso probatório absolutamente vedado, exceto se as comunicações encontradas estiverem inseridas no período compreendido por autorização judicial prévia que tenha sido regularmente concedida nos moldes da Lei nº 9.296/96, especialmente de seu artigo 5º.

Abstract: This article analyzes the secrecy of e-mail communication, of e-mail messages stored in the defendant's or its internet provider's hard disks, and of communications traffic data (also called external or non-human communication data). In such analysis, in order to define if those communications methods

[61] MENDES; COELHO; BRANCO. 2008, p. 306.

and types of traffic data are protected under the constitutional right to secrecy of communications (art. 5º, XII of Brazilian Constitution), the author considers international human rights conventions and their interpretation given and adopted by regional human rights courts, and, as criteria and methods, the principle of proportionality, and the doctrinally conceived standards for the construction of a criminal procedure system closer to an objective of efficiency and fundamental individual rights protection.

Keywords: Right to secrecy of communications. E-mail surveillance. Monitoring. Wiretapping. Eavesdropping of electronic communications. Seizure of stored e-mails. Communications traffic data.

Resumen: En este artículo se analiza el sigilo de la comunicación por correo electrónico, de los mensajes de correo electrónico almacenados en el disco duro del demandado o de su proveedor de Internet, y de los datos de tráfico de las comunicaciones (también llamados datos externos o no humano). En dicho análisis, con la finalidad de definir si esos métodos de comunicación y tipos de datos de tráfico están protegidos por el derecho constitucional al sigilo de las comunicaciones (art. 5º, XII de la Constitución brasileña), el autor considera las convenciones internacionales de derechos humanos y su interpretación dada y adoptada por los tribunales regionales de derechos humanos, y, como criterios y métodos, el principio de proporcionalidad, y las normas doctrinalmente concebidas para la construcción de un sistema procesal penal más cerca de un objetivo de eficiencia y garantismo.

Palabras clave: Derecho constitucional al sigilo de las comunicaciones. Aprehensión de correos electrónicos almacenados. Datos de tráfico de comunicaciones.

Referências

ALEXY, Robert. *Teoria dos direitos fundamentais*. Tradução Virgílio Afonso da Silva. 2. ed. São Paulo: Malheiros, 2011.

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.

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.

_____. 13ª Vara Federal de Curitiba. Decisão em pedido de quebra de sigilo telefônico nº 5049597-93.2013.404.7000/PR, 26.11.2013, p. 50 dos autos eletrônicos.

_____. 13ª Vara Federal de Curitiba. Representação de autoridade policial pela prorrogação de monitoramento nos autos 5049597-93.2013.404.7000/PR, 24.02.2014, p. 768 dos autos eletrônicos.

CANOTILHO, José Joaquim Gomes. *Direito constitucional e teoria da Constituição*. 7. ed. Coimbra: Almedina, 2000.

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: 31 jul. 2015.

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 maio 2013.

_____. Tribunal Supremo. Sala de lo Penal. STS 1550/2010. Recurso de 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 maio 2013.

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.

_____. 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 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.

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.

_____. 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.

_____. *Processo penal constitucional*. 6. ed. São Paulo: Revista dos Tribunais, 2010.

_____. 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.

FERRAZ JR., Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. In: *Revista da Faculdade de Direito da Universidade de São Paulo*, São Paulo, v. 88, p. 439-459, jan./dez. 1993.

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.

GRINOVER, Ada Pellegrini. *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*. 11. ed. São Paulo: Revista dos Tribunais, 2009.

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.

LOPES JR., Aury. *Direito processual penal e sua conformidade constitucional*. 3. ed. v. I. 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.

MENDES, Gilmar Ferreira; COELHO, Inocêncio Mártires; BRANCO, Paulo Gustavo Gonet. *Curso de direito constitucional*. 2. ed. rev. e atual. São Paulo: Saraiva, 2008.

MÜLLER, Friedrich. *Die Positivität der Grundrechte*: Fragen einer praktischen Grundrechtsdogmatik. 2. ed. Berlin: Duncker & Humblot, 1990.

MÜLLER, Friedrich. *Freiheit der Kunst als Problem der Grundrechtsdogmatik*. Berlin: Duncker & Humblot, 1969.

PRADO, Geraldo. *Limite às interceptações telefônicas e a jurisprudência do Superior Tribunal de Justiça*. 2. ed. Rio de Janeiro: Lumen Juris, 2006.

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

SILVA, Virgílio Afonso da. *Direitos fundamentais*: conteúdo essencial, restrições e eficácia. 2. ed. São Paulo: Malheiros, 2010.

TONINI, Paolo. *La prova penale*. 4. ed. Padova: Cedam, 2000.

TRIBUNAL EUROPEU DE DIREITOS HUMANOS. *Caso Calogero Diana vs. Itália*. Disponível em: <http://hudoc.echr.coe.int/eng?i=001-58072>. Acesso em: 01 ago. 2015.

_____. *Caso Kopp vs. Suíça*. Disponível em: <http://hudoc.echr.coe.int/eng?i=001-58144>. Acesso em: 01 ago. 2015.

TUTORIALSPOINT. Disponível em: <http://www.tutorialspoint.com/>. Acesso em: 30 ago. 2013.

WIRELESS DICTIONARY. Disponível em: <http://www.wirelessdictionary.com/Wireless-Dictionary-International-Mobile-Equipment-Identifier-IMEI-Definition.html>. Acesso em: 05 set. 2013.

Informação bibliográfica deste texto, conforme a NBR 6023:2002 da Associação Brasileira de Normas Técnicas (ABNT):

SIDI, Ricardo. A interceptação de *e-mails* e a apreensão física de *e-mails* armazenados. *Revista Fórum de Ciências Criminais – RFCC*, Belo Horizonte, ano 2, n. 4, p. 101-121, jul./dez. 2015.