Instituto dos Advogados Brasileiros

Av. Marechal Câmara, 210 - 3º andar - 20020-050 Tels.: (21) 2240-3921/2240-3173

www.ialnacional.org.br ial@ialnacional.org.br

Comissão de Direito Penal

Indicação 050/2022

Indicante: Márcio Gaspar Barandier

Matéria: Parecer sobre o Decreto Legislativo nº 37/2021, publicado no DOU de 17/12/2021, republicado em 21/12/2021, que aprovou o texto da Convenção sobre Crime Cibernético, celebrada em Budapeste, em 23 de novembro de 2001.

Ementa: Convenção sobre Crime Cibernético, celebrada em Budapeste em 2001. Conselho da Europa. Convite para a adesão do Brasil. Submissão do texto ao Poder Legislativo. Decreto Legislativo 37/2021. Aprovação do texto da convenção pelo Parlamento. Cooperação internacional para o combate ao crime cibernético. Tipificação de condutas. Procedimentos para a obtenção de dados. Cooperação internacional. Extradição. Assistência mútua em matéria penal.

Palavras-chave. Direito Internacional Público. Direito Penal. Direito Processual Penal. Cooperação internacional. Crimes cibernéticos. Procedimentos. Extradição. Assistência mútua.

Antes mundo era pequeno
Porque Terra era grande
Hoje mundo é muito grande
Porque Terra é pequena
Do tamanho da antena
Parabolicamará
Ê volta do mundo, camará
Ê, ê, mundo dá volta, camará
Antes longe era distante
Perto só quando dava
Quando muito ali defronte
E o horizonte acabava
Hoje lá trás dos montes
Dendê em casa camará
Gilberto Gil[1]

[1] GIL, Gilberto. Parabolicamará. Gege Edições/Preta Music. 1991. Site oficial.

Instituto dos Advogados Brasileiros

Av. Marechal Câmara, 210 - 3º andar - 20020-050 Tels.: (21) 2240-3921/2240-3173

www.ialnacional.org.br ial@ialnacional.org.br

Senhor Presidente,

Os versos iniciais da canção de Gilberto Gil, Parabolicamará, gravada no início da última década do século passado, revelam a provocação desse visionário poeta ao impacto das tecnologias na percepção do que se considerava mundo e globo terrestre. O mundo não poderia mais ser considerado pequeno, pois o horizonte havia se alargado tremendamente, muito além de trás dos montes.

Lá se vão mais de trinta anos desde que a música foi lançada no álbum homônimo. Desde então, a globalização anunciada na canção rompeu limites inimagináveis com a massificação do uso da internet. Hoje em dia, é difícil conceber como era a vida antes da disseminação da ferramenta. A internet está presente em tudo e se tornou imprescindível para a comunicação, o trabalho, a socialização, a obtenção de informações, os negócios, a administração pública, a medicina, enfim, para a maior parte das atividades humanas.

Como não poderia deixar de ser, as facilidades proporcionadas pela rede mundial de computadores também concorreram para o desenvolvimento de práticas criminosas, seja pelo uso da internet como instrumento do delito ou como local do desenvolvimento da própria atividade ilícita.

É impossível ignorar o expressivo número das mais diversas infrações penais cometidas na rede mundial de computadores, englobando desde ações criminosas com menor potencial ofensivo, como os delitos contra a honra, passando pelas fraudes, pelas notícias falsas, pelo preconceito racial, chegando até a crimes gravíssimos como homicídios e a prática de terrorismo.

O Decreto Legislativo nº 37/2021[2], publicado no DOU de 17/12/2021, republicado em 21/12/2021, aprovou o texto da Convenção sobre Crime Cibernético[3], celebrada em

[2] BRASIL Decreto legislativo 37/2021. Acesso em 23 de agosto de 2022 https://legis.senado.leg.br/norma/35289207/publicacao/35300588

[3] BRASIL PDL 255/2021 Acesso em 02 de março de 2022 https://legis.senado.leg.br/sdleg-getter/documento?dm=9026819&ts=1656678500768&disposition=inline

Budapeste, em 23 de novembro de 2001. O texto convencional foi negociado e firmado no âmbito do Conselho da Europa com a previsão de outros países poderiam ser convidados a aderir à convenção, como já ocorreu com a Argentina, Chile, Estados Unidos e outros mais.

O Brasil foi convidado para ser parte da Convenção e essa proposta foi aceita pela Presidência da República que cuidou de encaminhar o texto convencional ao Parlamento brasileiro para a necessária aprovação.

Após sua tramitação nas duas casas legislativas, foi editado o decreto legislativo já mencionado e, no presente momento, o texto aguarda a ratificação da Presidência da República, ato privativo e discricionário do mandatário da nação "pelo qual este confirma às outras partes, em caráter definitivo, a disposição do Estado de cumprir o tratado"[4].

A Convenção tipifica como crime diversas condutas praticadas contra a confidencialidade, a integridade e a disponibilidade de sistemas e contra os dados de computador e de tráfego, assim como define os crimes informáticos e as infrações penais relacionadas ao conteúdo da informação, como pornografia infantil, violação de direitos autorais e de direitos correlatos.

Há disposições procedimentais relacionadas a investigações e a processos criminais atinentes aos crimes tipificados na convenção, a outros crimes cometidos por meio de um sistema de computador e para coleta de provas eletrônicas da prática de qualquer outra espécie de crime.

A Convenção também estabelece normas de jurisdição, de cooperação internacional, de extradição e de assistência mútua em matéria penal, substrato que constitui o centro das atenções do presente trabalho.

Na compreensão dos subscritores do texto encaminhado à Presidência da República, a adesão à Convenção de Budapeste "proporcionará às autoridades brasileiras

[4] ARAÚJO, Nádia. Direito internacional privado, teoria e prática brasileira. São Paulo: Editora Revista dos Tribunais: 2020 https://proview.thomsonreuters.com/title.html?redirect=true&titleKey=rt%2Fmonografias%2F144455766%2Fv9.2&titleStage=F&titleAcct=e04ad7 acesso em 18/02/2022.

acesso mais ágil a provas eletrônicas sob jurisdição estrangeira, além de mais efetiva cooperação jurídica internacional voltada à persecução penal dos crimes cibernéticos[5]".

Segundo se vê no preambulo da Convenção, o seu objetivo é o de fomentar a cooperação entre os estados signatários do instrumento, mediante a criação de uma política criminal comum de combate aos crimes cibernéticos e a implementação na legislação interna de cada Parte de medidas que facilitem "a descoberta, a investigação e o julgamento dessas infrações penais em instâncias penais domésticas e internacionais" estabelecendo "mecanismos para uma cooperação rápida e confiável"[6].

Por outro lado, a convenção afirma ter assegurado o exercício da investigação e da persecução penal de forma equilibrada com os direitos humanos fundamentais, como a liberdade de consciência, a liberdade de expressão, os direitos à intimidade e à privacidade e à proteção dos dados pessoais.

A Convenção preconiza que as Partes adotem medidas a serem adotadas nas jurisdições nacionais (Capítulo II), bem como procedimentos de cooperação internacional (Capítulo III).

A primeira seção do Capítulo II do diploma convencional trata da tipificação de condutas que atentam contra a confidencialidade, a integridade, a disponibilidade dos dados e dos sistemas de computador, os crimes informáticos, a pornografia infantil e a violação de direitos autorais e de direitos correlatos. A norma internacional também sugere que a tentativa, o auxílio, a instigação e a incitação sejam também punidas como infrações penais, além de recomendar a responsabilização criminal das pessoas jurídicas pelos delitos tipificados pela Convenção.

A segunda seção do Capítulo II da Convenção de Budapeste dispõe sobre a aplicação de dispositivos processuais, ao tempo em que assinala que esses instrumentos deverão observar as condições e as garantias instituídas na legislação interna da Parte,

[5]BRASIL Senado Federal PDL 255/2021 https://legis.senado.leg.br/sdleg-getter/documento?dm=9026819&ts=1656678500768&disposition=inline

[6] BRASIL Senado Federal PDL 255/2021https://legis.senado.leg.br/sdleg-getter/documento?dm=9026819&ts=1656678500768&disposition=inline

com a adequada proteção aos direitos humanos e às liberdades públicas e com a incorporação do princípio da proporcionalidade. Dentre essas garantias, a convenção recomenda a adoção de controle judicial ou de supervisão independente sobre os procedimentos nela estabelecidos, exige fundamentação adequada, estabelece a limitação do âmbito de aplicação das medidas e fixa prazo certo para seu cumprimento.

O Capítulo III da Convenção de Budapeste aborda os princípios gerais da cooperação internacional e, na sequência, especifica os princípios aplicáveis à extradição e à assistência mútua, todos eles relacionados a assuntos penais, às condutas tipificadas de acordo como os artigos 2 a 11 da Convenção, às investigações e aos procedimentos relativos a essas infrações penais ou para a obtenção de provas eletrônicas de crimes.

1. As disposições penais da Convenção de Budapeste

Nesta parte do parecer analisaremos as propostas de criminalização da Convenção de Budapeste. Diferentemente de propostas legislativas internas, documentos internacionais que fazem sugestão de condutas a serem criminalizadas estabelecem um campo geral das mesmas a partir de determinados objetivos antes de uma pormenorização da ação.

Assim, não se trata de analisar uma proposta que trate de um texto legislativo de preceito primário e secundário, senão de uma sugestão genérica de criminalização, que inclusive conta com tipificações já existentes em nossa legislação.

Indica-se a leitura de nosso parecer a partir da topografia da Convenção e das legislações penais em vigência no Brasil que são correlatas às sugestões trazidas.

O título 1 da seção 1 do Capítulo II da Convenção é denominado “Crimes contra a confidencialidade, integridade e disponibilidade de dados e sistemas do computador”, indicando de forma expressa o bem jurídico tutelado pelos artigos 2 a 6 daquela legislação internacional. São eles: artigo 2 – acesso ilegal; artigo 3 - interceptação ilícita; artigo 4 - violação de dados; artigo 5 – interferência em sistema”; e artigo 6 - uso indevido de aparelhagem.

O título seguinte trata das infrações relacionadas com computadores, quais sejam: o Artigo 7 - Falsificação informática; e o Artigo 8 – Fraude informática.

Os artigos acima mencionados dão conta de atividades delituosas que já fazem parte do diploma criminal do Brasil, em especial pelas inclusões das Leis 12.737/2012 e 14.155/2021, notadamente do tipo "Invasão de dispositivo informático", no art. 154-A do Código Penal e de toda sua estrutura legal.

Este artigo delineia todas as questões trazidas pela Convenção haja vista a literalidade das preocupações externadas, tanto do ponto de vista de condutas como do ponto de vista de reprovações específicas no que tange o acesso, a interceptação, a violação, a interferência, o uso indevido de aparelhagem, a falsificação informática e a fraude informática.

Abaixo, reproduz-se tal estrutura, com destaque ao *caput* e aos § 1º, 2º, 3º e 4º, transcrevendo-se apenas os preceitos primários que tratam detidamente do objeto de nosso parecer:

> **Invasão de dispositivo informático**
>
> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
>
> (...)
>
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
>
> § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico.
>
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
>
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

A figura penal descrita no artigo 9 da Convenção também já está contemplada em nosso ordenamento jurídico, notadamente nos arts. 240 e 241 do Estatuto da Criança e do Adolescente, adicionada pela Lei 11.829/2008.

Enquanto a Convenção propõe a criminalização de condutas que estão descritas nos artigos do ECA apenas na modalidade "virtual", ou seja, quando o meio pelo qual as ações se dão é através de sistemas de computador, a amplitude já tipificada no Brasil abarca tais sugestões.

As infrações relacionadas com a violação do direito de autor e direitos conexos estão previstas no artigo 10 da Convenção. De igual forma, essa modalidade de conduta criminosa já é contemplada pelos artigo 184 do Código Penal e pelos artigos presentes no Título V "Dos Crimes contra a Propriedade Industrial" da Lei 9.279/1996. Apesar do artigo 10 da Convenção de Budapeste mencionar "Violação de direitos autorais e correlatos", a descrição do artigo menciona o "Acordo sobre Aspectos Comerciais da Propriedade Intelectual", o que abarca os outros tipos de propriedade intelectual, não apenas os relativos à proteção autoral.

Ao abordar as propostas legislativas acerca da tentativa, do auxílio ou da instigação a Convenção de Budapeste deixa em aberto, a título de interpretação, se há a vontade ou não de tipificações próprias de "tentativa", "auxílio" ou "instigação" para cada crime indicado pelos artigos anteriores.

Todavia, seja pela interpretação de que se indica apenas a necessidade dos países participantes de já preverem criminalizações de tais modalidades, seja de parte geral ou específica, fato é que o nosso ordenamento tem determinação geral sobre o tema.

Quanto a tentativa, tem-se o art. 14, II do Código Penal. Em relação ao auxílio ou à instigação, tem-se o art. 31 do Código Penal que determina os casos de impunibilidade, tratando estes dois últimos pontos como impuníveis caso não haja, pelo menos, a forma tentada do crime conexo, salvo disposições em contrário.

Parece-nos que tal posicionamento atual da norma deve se manter, em respeito ao Princípio da Reserva Legal e da Taxatividade, tanto pela perspectiva de que se não há

forma tentada dos crimes indicados neste parecer não há que se falar em criminalização de incitação e muito menos de auxílio.

Dessa forma, tem-se que não se deve adotar o item (1) do artigo 11 da Convenção, deixando claro desde já que o item (2) do mesmo artigo é facultativo a sua não adoção.

Para além de uma discussão mais profunda acerca da responsabilidade penal da pessoa jurídica, o artigo 12 da Convenção traz duas questões que não colidem com a realidade de ordenamento jurídico brasileiro:

> (1) Responsabilização criminal da pessoa natural pela conduta exercida.
>
> (2) No item 3. do r. artigo, apenas de seu título ser "Responsabilidade penal da pessoa jurídica", faculta-se que a responsabilidade pode ser civil ou administrativa, âmbitos já existentes em nosso ordenamento.

O artigo 13 da Convenção, em especial por todas as sugestões de criminalizações já estarem contempladas no ordenamento jurídico brasileiro, é perfeitamente aceitável, seja pela confirmação de sua disposição alternativa às sanções às Pessoas Jurídicas, seja por também abarcar o âmbito cível e administrativo.

Por outro lado, ao se referir ao compromisso que os países participantes têm em relação às sanções penais e às medidas legislativas, a norma dispõe de maneira cumulativa os critérios de eficácia, adequação e dissuasão indicada na locução "que incluam a privação de liberdade" que integra o dispositivo.

Aqui há de se indicar que a privação de liberdade não garante eficácia, adequação ou dissuasão de qualquer conduta, haja vista todo o acúmulo empírico do exercício do poder penal, qual seja, o aumento de penas ou o patamar destes a título de ensejar uma prisão em regime fechado não garante tais critérios.

Além do mais, a própria prática do poder penal indica ser propriamente problemática e multiplicadora de problemas sociais e econômicos a privação da liberdade em nosso país, tomando contorno próprio com o julgamento da liminar da ADPF 347 e o famigerado "estado de coisas inconstitucional" de nosso sistema penitenciário.

Apesar da maioria das condutas já criminalizadas ensejar a privação de liberdade, em diferentes modalidades de regime prisional, há que se ressaltar que o mesmo não ocorre no que tange às infrações contra os direitos autorais e conexos. Portanto, nesse caso há de ser reconhecida a inaplicabilidade do artigo 13 da Convenção, seja pelos motivos já esposados, seja pelos próprios critérios da Convenção.

2. Dos dispositivos processuais - Seções 2 e 3 da Convenção de Budapeste

Nesta seção do parecer, serão discutidas, sob o ângulo da constitucionalidade/legalidade, necessidade e conveniência, os aspectos processuais relativos à persecução penal e ao julgamento de crimes cibernéticos, previstos na Convenção de Budapeste.

A Seção 2 da referida Convenção é subdividida em: disposições gerais (Título 1, artigos 14 e 15); preservação expedita de dados armazenados em computador (Título 2, artigos 16 e 17); ordem de exibição (Título 3, art. 18); busca e apreensão de dados de computador (Título 4, art. 19); e obtenção de dados de computador em tempo real (Título 5, arts. 20 e 21). Como se vê, esta é a seção que elenca as medidas investigatórias e as regras gerais de sua aplicação.

Já a Seção 3 da Convenção de Budapeste é composta apenas pelo art. 22, que cuida de normas referentes à territorialidade e extraterritorialidade da lei penal de cada País aderente.

Como dito, o Título 1 da Seção 2 contempla as disposições gerais alusivas aos meios de obtenção das provas utilizáveis em investigações ou processos criminais (e as diretrizes normativas básicas para a implementação de cada um) a serem introduzidos no ordenamento jurídico do País que se dispuser a aderir à Convenção de Budapeste (v., neste particular, o art. 14.1).

Ressalvada a "interceptação de dados de conteúdo" (art. 21), cuja aplicabilidade a Convenção preconiza seja restrita a um rol exaustivo de crimes[7], os meios de obtenção de prova contemplados na Seção 2 se destinam não apenas à instrução de investigações e de processos pelos crimes cibernéticos, elencados nos artigos 2 a 11 da Convenção, mas também a "outros crimes cometidos por meio de um sistema de computador" (art. 14.2.b) e à "coleta de provas eletrônicas da prática de um crime" (art. 14.2.c), qualquer que seja o delito.

Parece conveniente e adequado que, uma vez introduzidas no ordenamento jurídico pátrio diligências investigatórias relacionadas a sistemas de computador, sua utilização não fique restrita aos crimes previstos na própria Convenção, mas também para toda e qualquer infração que venha a ser praticada por meio de um computador.

No caso de comunicações transmitidas por um provedor de serviço que "estiver sendo operado em benefício de um grupo fechado de usuários" e "não empregar redes públicas de comunicação" e tampouco esteja "conectado com outro sistema de computador, seja ele público ou privado", o art. 14.3.b da Convenção estabelece uma exceção.

Nessa hipótese, o Estado aderente que, por conta de eventuais "obstáculos legais" porventura existentes ao tempo da adesão à Convenção, se vir impossibilitado a aplicar as medidas dos artigos 20 e 21 ("obtenção de dados de computador em tempo real" e "interceptação de dados de conteúdo", respectivamente), poderá deixar de aplicar tais diligências investigatórias/instrutórias, mas ficará sujeito a que qualquer outro Estado aderente oponha óbice a reserva dessa espécie, "a fim de possibilitar a mais ampla aplicação das medidas referidas nos Artigos 20 e 21".

Cabe ressaltar que este dispositivo, pelo menos no presente momento, não encontra aplicabilidade no caso do Brasil, uma vez que inexistem impedimentos legais à

[7] No que se refere à diligência de "obtenção de dados de computador em tempo real", prevista no art. 20, a restrição de sua aplicabilidade a um conjunto de delitos específicos é **facultativa**, de acordo com o art. 14.3.a, desde que o rol de crimes eventualmente incluídos no raio de aplicabilidade da diligência probatória em questão "*não seja mais restrito do que o conjunto de crimes aos quais esse Estado aplica as medidas mencionadas no Artigo 21*".

interceptação ou obtenção de dados telemáticos, provenham estes do sistema de computador(es) de que provierem.

Ainda em sede de disposições gerais, o artigo 15.1 da Convenção subordina "o estabelecimento, a implementação e a aplicação" de todos os procedimentos probatórios elencados na Seção 2, sem exceção, à observância das condições e garantias individuais consagradas na legislação interna do Estado aderente, incluídas as garantias cristalizadas nos diplomas internacionais de direitos humanos, observado sempre o princípio da proporcionalidade. Dentre as garantias mínimas a serem observadas, contam-se o "controle judicial" (ou "supervisão independente"), a "fundamentação" da implementação da medida probatória e a "limitação do âmbito de aplicação e de duração" de tais procedimentos probatórios (cf. art. 15.2).

Neste particular, os preceitos gerais da Convenção de Budapeste são mais garantidores do que a legislação interna brasileira, ao menos no que diz respeito à necessidade de ordem judicial para acessar o conteúdo de sistemas de computador, a qual em alguma medida se ressente de regulamentação entre nós.

O ordenamento jurídico brasileiro tutela a inviolabilidade das comunicações realizadas por meio do computador e dos dados armazenados em dispositivos informáticos, havendo divergência na doutrina e na jurisprudência em relação ao fundamento constitucional da tutela jurídica no segundo caso.

Para a doutrina constitucionalista, a garantia do art. 5º, inc. XII, da Carta protege apenas o fluxo das comunicações (telefônicas e telemáticas), ao passo que a inviolabilidade dos dados armazenados em dispositivos informáticos encontra guarida constitucional no art. 5º, inc. X, da Carta de 1988[8]. Esse entendimento encontra alguma ressonância na jurisprudência, valendo citar, para fins de ilustração, o acórdão proferido no julgamento do RE 418.416, no qual o Pleno da Suprema Corte brasileira negou vigência

[8] Representativa, no âmbito da doutrina, dessa corrente são as lições de MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. Curso de Direito Constitucional, S.Paulo, 2019, Saraiva Educação, p. 300; e de SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. Curso de Direito Constitucional, S.Paulo, 2018, Saraiva Educação, p. 474.

ao art. 5º, inc. XII, numa hipótese em que houve "*apreensão de base física na qual se encontravam os dados* [telefônicos]*, mediante prévia e fundamentada decisão judicial*", porque "*a proteção a que se refere o art. 5º, XII, da Constituição, é da comunicação 'de dados' e não dos 'dados em si mesmos', ainda quando armazenados em computador*"[9].

Como se pode notar, embora o precedente não tenha versado especificamente sobre o acesso aos discos rígidos de computador (mas sim a registros telefônicos contidos em um aparelho celular), o raciocínio ali empregado tem força de expansão lógica para abranger os dados armazenados em quaisquer equipamentos informáticos.

Para a doutrina processual penal, contudo, tanto a comunicação telefônica ou de dados quanto os próprios dados armazenados em dispositivos informáticos (não capturados em cumprimento à diligência de interceptação) encontram tutela na garantia do art. 5º, inc. XII, da Lei Maior[10]. A referência ao art. 5º, inc. XII, transporta o tratamento infraconstitucional da questão para a lei 9.296/96, que, no entanto, não contém um dispositivo específico que exija autorização judicial para acessar dados armazenados no computador e não capturados pela interceptação, embora tal necessidade esteja consagrada pela práxis.

Subjaz à controvérsia, como se percebe, o regime jurídico aplicável ao acesso de dados armazenados em equipamentos de informática. É certo, por um lado, que a interceptação das comunicações de dados telemáticos deve observar os requisitos e o procedimento da lei 9.296/96, por força da remissão expressa que faz o seu art. 1º, par. único[11]. Este diploma, por sinal, positiva

---

[9] STF, Tribunal Pleno, RE 418.416, rel. Min. Sepúlveda Pertence, j. 10.mai.06, DJ 19.dez.06.

[10] É o que sustentam, entre outros, TUCCI, Rogério Lauria. Direitos e Garantias Individuais no Processo Penal Brasileiro, S.Paulo, 2004, Saraiva, p. 405; MACHADO, André Augusto Mandes; KEHDI, Andre Pires de Andrade. *Sigilo das comunicações e de dados*. *In* FERNANDES, Antonio Scarance; ALMEIDA, José Raul Gavião de; MORAES, Maurício Zanoide de (orgs.). Sigilo no Processo Penal – Eficiência e Garantismo. S.Paulo, 2008, ed. RT, p. 243; e SIDI, Ricardo. A Interceptação das Comunicações Telemáticas no Processo Penal, B.Horizonte, 2016, Ed. D'Plácido, p. 306.

[11] Convém registrar a controvérsia que gira em torno da possível inconstitucionalidade do art. 1º, par ún., da lei 9.296/96, mercê das interpretações dadas ao alcance da garantia fundamental do art. 5º, inc. XII, da CF ("*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*"). Não será importante, aqui, conhecer os pormenores dessa polêmica; baste-nos registrar que predomina o entendimento assim enunciado por Streck: "*não vislumbro inconstitucionalidade no dispositivo sob comento*", à medida que "*o parágrafo único* [do art. 1º]*, ao estender a possibilidade de interceptação também ao fluxo de comunicações em sistemas de informática e telemática, apenas especificou que a lei também atingirá toda e qualquer variante de informações que utilizem a modalidade 'comunicações telefônicas'*" (STRECK, Lenio Luiz. As Interceptações Telefônicas e os Direitos Fundamentais, P.Alegre, 2001, Livr. do Advogado, p. 46).

os mecanismos de reforço da tutela constitucional da privacidade/intimidade que o art. 15.1 da Convenção de Budapeste recomenda aos Estados aderentes: ordem judicial fundamentada (art. 1º, *caput* c/c art. 5º), demonstração da necessidade (art. 2º, inc. II c/c art. 4º) e limitação do âmbito de aplicação e de duração (art. 2º, par. ún. c/c art. 5º). Mas como a lei 9.296/96 se refere apenas à interceptação telemática de dados de conteúdo, o acesso a dados de conteúdo armazenados no computador fora das situações de interceptação fica inevitavelmente subordinado à disciplina da busca e apreensão.

A teor do art. 5º, inc. XI, da Carta de 1988, a busca domiciliar só pode ser efetivada quando antecedida de ordem judicial (cf. art. 5º, inc. XI, CF), que deve indicar o *fumus boni iuris*, consistente em fundadas razões que indiquem a ocorrência de pelo menos uma das finalidades legais (cf. art. 240, § 1º e alíneas, CPP), e o *periculum in mora*, "*evidenciado pela necessidade de se colher, o mais rapidamente possível, os elementos probatórios que interessam ao esclarecimento dos fatos discutidos no processo*", segundo a dicção de Campos Tôrres[12]. Além disso, a decisão deve indicar, com a maior precisão possível, o local da diligência (art. 243, incs. I e II, CPP).

Já a busca pessoal pode ser realizada sem ordem judicial prévia "no caso de prisão ou quando houver fundada suspeita de que a pessoa esteja na posse de arma proibida ou de objetos ou papeis que constituam corpo de delito, ou quando a medida for determinada no curso de busca domiciliar" (art. 244 CPP). Se não há muita dúvida quanto à possibilidade de que a autoridade policial, na execução de busca pessoal, apreenda o dispositivo que armazena (ou dá acesso aos provedores que armazenam) os dados telemáticos mesmo à míngua de ordem judicial prévia, no que se refere à devassa do conteúdo do dispositivo informático porventura apreendido a situação já não é tão simples.

Neste particular, a polêmica que orbita o alcance da garantia do art. 5º, inc. XII, da Carta Política, somada à já citada falta de regramento infraconstitucional específico, lança considerável insegurança jurídica no que se refere à licitude da devassa, sem permissão judicial prévia, do conteúdo de dispositivos portáteis que armazenam dados telemáticos (notebooks, *tablets* ou aparelhos de telefonia celular) que estejam na posse do indivíduo eventualmente submetido à busca pessoal. A propósito, o art. 19.5 da Convenção de Budapeste exige ordem judicial para toda

[12] TÔRRES, Ana Maria Campos. A Busca e Apreensão e o Devido Processo Legal, Rio, 2004, Forense, p. 112. Bastos Pitombo acrescenta que as finalidades previstas no art. 6º, incs. II e III, do CPP são "*dominadas, também, pela urgência*" (Da Busca e Apreensão no Processo Penal, S.Paulo, 2005, ed. RT, p. 114).

e qualquer busca e apreensão de dados de computador, sem distinção entre busca domiciliar ou pessoal, o que fará com que, finalmente, a garantia fundamental da reserva de jurisdição no que se refere ao acesso ao conteúdo de um sistema de computador em seguida a uma busca pessoal executada sem ordem judicial prévia, ganhe a necessária proteção infraconstitucional entre nós.

A diligência de "preservação expedita", tratada nos artigos 16 e 17 da Convenção, consiste na expedição de uma ordem direcionada à pessoa que tenha sob sua posse, detenção ou controle "dados de computador determinados" (art. 16.2), "incluindo dados de tráfego" (art. 16.1), para que preserve e mantenha "a integridade desses dados de computador pelo período de tempo necessário" (art. 16.2), de maneira a permitir à autoridade competente buscar sua revelação. A preservação será determinada pelo prazo necessário, "até o máximo de 90 (noventa) dias", ressalvada a possibilidade de renovação subsequente da ordem (art. 16.2).

No que se refere especificamente a dados de tráfego, o Estado signatário da Convenção deve assegurar que a ordem de preservação seja cumprida "independentemente do número de provedores de serviço envolvidos na transmissão dessa comunicação" (art. 17.1.a) e de maneira que assegure "expedita revelação à autoridade competente da Parte", ou a uma pessoa por ela indicada, de "um conjunto suficiente de dados de tráfego" que permitam identificar os provedores de serviço e o "caminho por meio do qual a comunicação se realizou" (art. 17.1.b).

Em todo caso, o Estado-Parte deverá tomar providências legislativas (e/ou de outra natureza) para obrigar que o destinatário da ordem de preservação (detentor dos dados ou terceiro encarregado da sua preservação) mantenha em sigilo, por um período de tempo a ser estabelecido na legislação interna, "o início do procedimento investigativo" (art. 17.3). A imposição de sigilo é justificada pelo desiderato de evitar que haja manipulação, adulteração ou supressão dos dados que podem interessar à investigação.

Como se nota, nessa seção 2 a Convenção de Budapeste institui uma medida cautelar probatória preventiva, que tem por objetivo assegurar a preservação do *corpus delicti*. É uma medida menos invasiva do que a busca e apreensão, que é o instrumento que o Código de Processo Penal destina para a finalidade de reunir o *corpus delicti* (v., a propósito, alíneas "b" a "f" e "h" do § 1º do art. 240 CPP), porque envolve tão-somente a preservação eletrônica dos dados, não exigindo o ingresso da Polícia e/ou Oficial de Justiça no domicílio do investigado nem a apreensão de computadores, *smartphones*, *tablets* etc.

Vale salientar que o artigo 13 da lei 12.965/14, que regulamenta o uso da internet no Brasil, estabelece *ex-lege* a obrigatoriedade de manutenção dos registros de conexão imposta aos provedores de serviço na rede mundial de computadores, pelo prazo de um ano, o qual pode ser elastecido em atenção a requerimento cautelar de autoridade policial ou administrativa, ou do Ministério Público.

Além disso, o Marco Civil da Internet prevê a possibilidade de que a Autoridade Judiciária ordene "ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet", que a Convenção de Budapeste chama de "dados de tráfego" (cf. art. 1.d), para a finalidade de "formar conjunto probatório em processo judicial cível ou penal" (art. 22). A lei 12.965/14, contudo, não prevê uma medida que se limite apenas a determinar a preservação dos dados de computador (dados de tráfego e de conteúdo humano), para posterior entrega ao Estado-parte.

Portanto, não se vislumbra nenhum atentado ao ordenamento jurídico interno na medida prevista no art. 16 da Convenção de Budapeste, pois já contemplada pela legislação doméstica brasileira.

Por outro lado, é de se salientar que a previsão de observância dos arts. 14 e 15 da Convenção de Budapeste (cf. art. 17.2), isto é, a imposição de ordem judicial, de respeito aos direitos e garantias individuais, de estabelecimento de limites para a aplicação da medida cautelar em comento, entre outras, se compatibiliza com os requisitos que o art. 22, parágrafo único, da lei 12.965/14, impõe para o fornecimento de dados de tráfego de usuários da internet, a saber: fundados indícios da ocorrência do ilícito (inc. I), justificativa motivada da utilidade dos registros solicitados (inc. II) e delimitação do período ao qual se referem os registros (inc. III).

No entanto, o texto da Convenção de Budapeste é lacônico quanto à ordem de "preservação expedita" poder ser direcionada ao próprio investigado/indiciado/acusado. Seria conveniente que ficasse clara a impossibilidade, uma vez que o ordenamento jurídico brasileiro é regido, entre outras, pela regra da proteção contra a autoincriminação. Além de garantir expressamente ao indivíduo preso o direito ao silêncio (art. 5º, inc. LXIII) e o respeito à integridade física e moral (art. 5º, inc. XLIX), a Constituição da República assegura aos acusados em geral a garantia da ampla defesa (art. 5º, inc. LV).

Desse plexo de garantias, decorre a regra segundo a qual "não podem ser aplicadas ao acusado medidas atentatórias à sua [do acusado] integridade física e moral, incluindo-se as que objetivam sua cooperação na persecução penal"[13].

Complementa Haddad aduzindo que a busca e apreensão se justifica precisamente porque "o acusado não está obrigado a produzir ou a entregar provas incriminatórias"[14]. A Suprema Corte brasileira tem posição firmada no sentido de que "o direito de não produzir prova contra si mesmo, ao relativizar o dogma da verdade real, garante ao investigado os direitos de nada aduzir quanto ao mérito da pretensão acusatória e de não ser compelido a produzir ou contribuir com a formação de prova contrária ao seu interesse, ambos pilares das garantias fundamentais do direito ao silêncio e do direito à não autoincriminação"[15].

A "Ordem de exibição", prevista no artigo 18 do diploma internacional, é a locução que designa a medida destinada a ordenar: a) "a qualquer pessoa residente em seu território a entregar dados de computador especificados, por ela controlados ou detidos, que estejam armazenados num sistema de computador ou em qualquer meio de armazenamento de dados de computador" (art. 18.1.a); e b) "a qualquer provedor de serviço que atue no território da Parte a entregar informações cadastrais de assinantes de tais serviços, que estejam sob a detenção ou controle do provedor" (art. 18.1.b).

Ressalvada a impossibilidade de que tal "ordem de exibição" seja direcionada ao próprio investigado/indiciado/acusado, pelos motivos expostos linhas acima, nada há a objetar em relação a essa diligência, que visa a complementar a "preservação expedita" vista no item precedente.

Por um lado, o § 5º do artigo 13 e o art. 22 da lei 12.965/14 já contemplam a obrigatoriedade de preservação e de entrega de dados relativos ao uso da internet; por outro lado, a busca e apreensão (ou seja, o apossamento *inaudita altera pars*, ainda que temporário, dos referidos dados pelas autoridades de persecução penal) já são largamente utilizadas como instrumentos para a obtenção de dados armazenados nos discos rígidos dos computadores.

A busca e a apreensão são diligências de obtenção de prova que desfrutam de larga tradição na legislação processual brasileira. Assim, seria de questionável necessidade a introdução de um dispositivo, como o art. 19 da Convenção, ora examinado, que buscasse "dar poderes a suas

[13] QUEIJO, Maria Elizabeth. O Direito de Não Produzir Prova contra Si Mesmo, S.Paulo. 2003, Saraiva, p. 73,
[14] HADDAD, Carlos Henrique Borlido. Conteúdo e Contornos do Princípio contra a Auto-Incriminação, Campinas, 2005, Bookseller, p. 217.
[15] STF, Pleno, RE 971.959, rel. Min. Luiz Fux, j. 14.nov.18, DJe 31.jul.20.

autoridades competentes para busca ou investigação" dos dados armazenados em sistemas de computador.

A Convenção de Budapeste, no entanto, inova em dois aspectos. Em primeiro lugar, o art. 19.2 contempla a possibilidade de que a autoridade competente, ao proceder à busca em determinado sistema de computador, no momento em que "tiver fundadas razões para supor que os dados procurados estão armazenados em outro sistema de computador ou em parte dele" e perceber que "tais dados são legalmente acessíveis a partir do sistema inicial", estenda "prontamente", isto é, sem a necessidade de autorização judicial superveniente, a busca ao outro sistema, podendo apreender os dados buscados.

A segunda inovação vem no art. 19.3, que cuida da apreensão dos dados porventura encontrados. Diz a Convenção que devem se incluir no poder de apreensão dos dados eventualmente encontrados (cf. art. 19.3.a) os poderes alternativos de: (i) fazer e guardar uma cópia dos dados do computador que interessem à investigação ou processo (art. 19.3.b); (ii) manter a integridade dos dados de computador relevantes (art. 19.3.c); e (iii) tornar inacessíveis esses dados no sistema de computador acessado ou dele removê-los (art. 19.3.d). Nosso interesse gira em torno dos poderes de "manter a integridade dos dados" e de "tornar inacessíveis" tais dados.

Quanto à primeira inovação, a medida pretendida é de duvidosa constitucionalidade. No figurino tradicional da busca e apreensão, diz o Código de Processo Penal que o mandado de busca deverá "indicar, o mais precisamente possível, a casa em que será realizada a diligência e o nome do respectivo proprietário ou morador (...)" (art. 243, inc. I), bem como "mencionar o motivo e os fins da diligência" (inc. II).

Na dicção de Pitombo, isso significa que, "não pode haver mandado incerto, vago ou genérico"[16]. Portanto, se seria ilegal um mandado que autorizasse a autoridade policial a acessar "qualquer sistema de computador" (tal como é ilegal um mandado de busca e apreensão que autoriza o ingresso em qualquer casa de uma favela para apreensão de drogas e armas), independentemente de sua localização ou de quem é o proprietário/usuário.

Deste modo, parece bastante evidente a impossibilidade de que a autoridade policial o faça sem autorização judicial específica, especialmente se a coisa buscada não é determinada (como, por exemplo, na situação em que o mandado menciona "qualquer arquivo de vídeo, de imagem ou assemelhado que contenha pornografia infantil) e se o segundo sistema de

[16] PITOMBO, Cleunice Bastos. Da Busca e Apreensão no Processo Penal, S.Paulo, 2005, ed. RT, p. 205.

computador, a ser acessado a partir do primeiro, pertença a pessoa distinta daquela que foi o alvo originário da busca e apreensão. Essa previsão acaba por esvaziar a garantia da reserva de jurisdição.

A previsão de se "manter a integridade dos dados" (art. 19.3.c) gera uma certa estranheza, pois não se entende qual poderia ser a alternativa, pelo menos enquanto perdurar a persecução penal. A não-manutenção da integridade dos dados significa a quebra da cadeia de custódia da prova (art. 158-B, inc. IX, CPP), que leva à invalidade desta. Se o descarte dos dados ocorrer antes que o investigado/indiciado/acusado tenha tido a oportunidade de se manifestar sobre a realização de contraperícia ou de solicitar esclarecimentos aos peritos que os tenham examinado, a quebra da cadeia de custódia se traduzirá em nulidade do processo. Uma vez encerrada a persecução penal, pode haver o descarte dos dados, desde que caracterizada alguma das situações de perdimento de bens, previstas no art. 91, inc. II, do CP.

No que tange a "tornar inacessíveis" ou remover os dados ou arquivos apreendidos do sistema de computador nos quais foram apreendidos, entende-se justificada a medida apenas e tão-somente se o material apreendido constituir instrumento ou produto do crime (no primeiro caso, quando se tratar de arquivo cuja mera detenção já constitua fato ilícito, cf. art. 91, inc. II, al. "a", CP), que são objeto de perdimento uma vez encerrada a persecução penal, nos termos do já citado art. 91, inc. II, do CP.

Não se encontra semelhante justificativa quando o arquivo, dado ou informação em questão constituírem apenas uma prova do cometimento da infração. A regra, portanto, deve ser a da acessibilidade dos dados por todas as partes envolvidas na persecução penal, muito especialmente o investigado/indiciado/acusado, que tem a lhe amparar neste particular a garantia constitucional da ampla defesa (art. 5º, inc. LV, CF).

Por fim, reitere-se o que a Convenção de Budapeste recomenda, para qualquer caso de busca e apreensão a necessidade de ordem judicial. Assim, será sanada a deficiência regulatória que se observa no ordenamento jurídico processual penal brasileiro, no caso do acesso aos dados armazenados em equipamento apreendido durante a diligência de busca pessoal. Não obstante a práxis judiciária revelar que essa espécie de acesso tem sido precedida de autorização judicial, o fato inconteste é o de que esse cuidado decorre da interpretação de dispositivos de garantia previstos na Constituição da República e não do comando decorrente de dispositivo legal ordinário.

Na sequência, o artigo 20 da Convenção disciplina a diligência de obtenção, em tempo real, de dados de tráfego "vinculados a comunicações específicas" (art. 20.1). Essa obtenção, segundo a Convenção, pode ocorrer por meio da coleta e gravação direta de tais dados de tráfego, ou por meio de provedor do serviço de *internet*. Esta diligência é complementar em relação à interceptação de dados de conteúdo, de que a Convenção cuida no artigo subsequente (art. 21). A Convenção prevê, ainda, que o Estado-parte deverá adotar medidas legislativas (e de outras naturezas) para o fim de "obrigar um provedor de serviço a manter em sigilo a execução de qualquer das atribuições investigativas estabelecidas neste Artigo e quaisquer informações relativas a elas" (art. 20.3).

Se é possível a interceptação de dados de conteúdo – e no item seguinte veremos que é, pois a própria legislação atual já a autoriza – com mais razão pode haver a interceptação de dados de tráfego, que são os dados relacionadas à conexão (dia, hora de início e de término da conexão, endereço de IP etc.) do sistema de computador.

Ricardo Sidi usa uma pirâmide invertida para representar graficamente o grau crescente de interferência (e de volume trafegado) dos diferentes níveis de dados e informações na intimidade/privacidade do usuário do sistema de computador. Segundo a ilustração de Sidi, os dados cadastrais do usuário são aqueles sobre os quais repousa a menor expectativa de privacidade, ao passo que os dados de tráfego e os dados de conteúdo são aqueles nos quais, em ordem crescente, se deposita a maior expectativa de privacidade. Ambos, adiciona Sidi, constituem os tipos de dados "que poderemos situar dentro do âmbito de proteção do sigilo das comunicações"[17].

De pouca valia seria a interceptação de dados de conteúdo, como arquivos, fotos e vídeos, se não se pudesse dispor, com a mesma presteza, dos dados de tráfego. Não é preciso muito esforço para se perceber que os dados de tráfego guardam tanta importância para a investigação de ilícitos penais praticados por meio de um sistema de computador quanto os próprios dados de conteúdo transmitidos ou armazenados.

A bem da verdade, os dados de tráfego integram o corpo de delito, já que são inequivocamente vestígios da possível prática criminosa (cf. art. 158, *caput*, CPP) por indicarem as circunstâncias de tempo e lugar da transmissão de dados, o que é importante tanto para fins de prova da autoria quanto para o estabelecimento da competência, do prazo prescricional etc.

[17] SIDI, Ricardo. Op. Cit., p. 295.

Assim, não só não se vislumbra nenhuma colisão da Convenção de Budapeste com a legislação interna brasileira, como a providência ora examinada é de importância elementar para as finalidades perseguidas pela Convenção.

Concluamos o exame da diligência de "obtenção de dados de computador em tempo real" relembrando que o art. 14.3.a da Convenção diz ser facultativo que o Estado-parte restrinja sua aplicação a certos "crimes ou a categorias de crimes", desde que esse conjunto não seja mais restrito do que aquele previsto para a diligência que veremos na sequência, a interceptação de dados de conteúdo (art. 21 da Convenção). Neste particular, cumpre esclarecer que a lei 9.296/96 não distingue a interceptação de dados de tráfego da interceptação dos dados de conteúdo, sendo ambos os tipos de dados obtidos simultaneamente no curso da interceptação.

O último meio de obtenção de prova está contido no artigo 21 da Convenção de Budapeste. A interceptação de dados de conteúdo consiste no acesso, em tempo de real, de comunicações realizadas por meio de sistema de computador, sempre que houver a suspeita de prática de "um conjunto de crimes graves a serem especificados pela legislação doméstica" (art. 21.1).

De forma similar ao que ocorre com a diligência anterior, a Convenção de Budapeste determina a adoção de medidas legislativas voltadas a "obrigar um provedor de serviço a manter em sigilo a execução de qualquer das atribuições investigativas" previstas no próprio artigo 21, bem como no que diz respeito às próprias informações obtidas no curso da diligência, o que já é previsto em nossa legislação (cf. art. 1º, *caput*, da lei 9.296/96) e cuja necessidade e importância dispensam maiores comentários.

A lei 9.296/96 regula primordialmente a interceptação de comunicações telefônicas, assim como é aplicável "à interceptação do fluxo de comunicações em sistemas de informática e telemática" (art. 1º, par. único), restando contemplados todos os requisitos previstos na Convenção de Budapeste.

A aplicabilidade exclusiva "a um conjunto de crimes graves a serem especificados pela legislação doméstica" é refletida no art. 2º, inc. III da lei 9.296/96, que, a *contrario sensu*, restringe a utilização da interceptação apenas aos crimes punidos com reclusão. De resto, a lei 9.296/96 tem uma regulamentação bastante detalhada, que atende inteiramente ao quanto preconiza a Convenção de Budapeste.

Embora a terceira seção se intitule "Jurisdição", o art. 22 da Convenção de Budapeste, na verdade, versa sobre situações de territorialidade e extraterritorialidade da lei penal e processual penal do Estado-parte. Diz o referido artigo que cada Parte adotará medidas legislativas necessárias para estabelecer jurisdição sobre qualquer dos crimes tipificados nos arts. 2 a 11 da Convenção quando for cometido: a) no seu território, b) a bordo de uma embarcação de bandeira do Estado-parte, c) a bordo de aeronave registrada conforme as leis do Estado-parte e/ou d) por cidadão de nacionalidade do Estado-parte, salientando-se, neste último caso, que o crime seja punível segundo as leis penais do local do fato ou que tenha sido cometido fora da jurisdição de qualquer Estado-parte.

No que se refere ao primeiro caso – infração cometida no território do Estado-parte – o art. 5º, *caput*, do Código Penal já contempla referida regra: "aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional".

Quanto ao segundo e terceiro caso – infração praticada a bordo de embarcação e aeronave brasileira – o Código Penal, em seu art. 5º, § 1º, considera como extensão do território nacional (remetendo, portanto, à regra geral do *caput* do art. 5º, que consagra a aplicabilidade da lei penal brasileira) "as embarcações e aeronaves brasileiras, de natureza pública ou a serviço do governo brasileiro onde quer que se encontrem, bem como as aeronaves e embarcações brasileiras, mercantes ou de propriedade privada, que se achem, respectivamente, no espaço aéreo correspondente ou em alto-mar".

Quando o crime for cometido a bordo de embarcação ou aeronave brasileira, mercante ou de propriedade privada, que se encontre em território estrangeiro, nosso Código Penal contém uma hipótese de extraterritorialidade da lei penal brasileira (art. 7º, inc. II, al. "c"), que se subordina unicamente à condição de o fato não ser julgado no país estrangeiro em questão. Em suma, a legislação penal brasileira já atende ao que preceitua a Convenção de Budapeste.

Finalmente, no que se refere ao último caso – infração praticada (no estrangeiro) por brasileiro – nosso Código Penal contempla tal hipótese da extraterritorialidade no art. 7º, inc. II, al. "b". A primeira das condições previstas na Convenção de Budapeste para este caso específico – ser o fato punível no local em que praticado – está prevista também em nosso Código Penal como condição para aplicabilidade da lei penal brasileira (cf. art. 7º, § 2º, al. "b"). Quanto à segunda condição – crime cometido fora da jurisdição de qualquer Estado-parte – também se pode

considerar atendida: o brasileiro será punido pelo crime praticado no estrangeiro, desde que cumpridas as condições do § 2º do art. 7º do nosso Estatuto Penal.

3. Da Cooperação internacional – Capítulo III da Convenção de Budapeste

A Convenção estabeleceu os princípios regentes da cooperação internacional em seu artigo 23. Segundo estabelece o dispositivo, além das regras constantes do texto supranacional, também deve ser observada a aplicação de outros instrumentos internacionais de cooperação em assuntos penais e os acordos firmados com base em legislação uniforme ou na reciprocidade. A legislação interna de cada país também deverá ser levada em conta, restando assim reafirmada a soberania das nações signatárias da Convenção. Portanto, a ideia que permeia todo o texto é a de possibilitar a realização, sem empecilhos, de investigações ou de procedimentos relacionados aos crimes de computador tipificados na Convenção e facilitar a coleta de provas eletrônicas dessas infrações penais.

No tocante às normas de extradição, a Convenção condiciona a execução desse ato de cooperação à dupla tipificação da conduta criminosa, na forma dos seus artigos 2 a 11, e que ela seja punível com pena privativa da liberdade de pelo menos um ano, como se vê no artigo 24.1a da Convenção. A exceção a essa regra pode ocorrer quando um acordo de legislação uniforme, de reciprocidade ou tratado de extradição estabelecer uma pena mínima diferente.

Os autores dos delitos tipificados pela Convenção poderão ser extraditados ainda que ainda que não exista convenção de extradição entre os Estados-Parte, servindo a Convenção como base legal da pretendida extradição, podendo a Parte requerida exigir o cumprimento de condições estabelecidas por sua legislação ou até recusar a extradição, se assim dispuser a sua legislação. Se a recusa estiver fundada apenas na nacionalidade da pessoa ou por se a Parte requerida considerar ter jurisdição sobre o fato, ela deverá submeter o pedido a suas autoridades para a persecução penal segunda a legislação interna aplicável.

Ao seu turno, os princípios gerais da assistência mútua relacionados à elucidação e à persecução dos denominados crimes cibernéticos previstos na Convenção, assim como os atinentes à obtenção de provas eletrônicas de crimes comuns estão previstos no artigo 25 da Convenção de Budapeste. Segundo esse dispositivo, os signatários e os aderentes da Convenção assumem o compromisso de adotar as medidas legislativas que permitirão maior celeridade aos pedidos de assistência, os quais poderão ser formulados por meios de comunicação rápida, como fax e e-mail, nos casos em que houver urgência na obtenção dos dados solicitados.

A assistência mútua sempre estará sujeita à observância da legislação interna de cada país. No entanto, a assistência não poderá ser recusada ao argumento de que a conduta à qual se refere o pedido for considerada um simples delito financeiro. Por outro lado, a assistência mútua pode estar condicionada à existência de dupla tipicidade para os delitos não tipificados na convenção, pouco importando se for diversa a denominação dada à conduta criminosa, desde que seja caracterizada como infração penal.

O direito de recusar o pedido também poderá ser exercido quando a infração penal que fundamenta a assistência mútua for considerada como crime político, ou conexo, pela Parte requerida. Também é possível a recusa quando ela entender que a execução do pedido compromete a sua soberania, segurança, ordem pública ou outro interesse essencial. A Parte requerente será prontamente informada das razões de recusa, do retardo do pedido de assistência, ou quando for oponível alguma condição para sua execução.

A Convenção de Budapeste também prevê que as suas disposições não serão aplicáveis quando houver tratados de assistência mútua, de acordos de legislação uniforme ou de reciprocidade entre as Partes requerida e requerente. Contudo, se houver consenso, essas Partes podem preferir aplicar os dispositivos de assistência mútua previstos na Convenção, no todo ou em parte, e não os instrumentos previstos nos outros acordos.

Em regra, os pedidos de assistência mútua serão executados por uma autoridade central ou encaminhados à autoridade competente para cumpri-los. O nome e o endereço

da autoridade central de cada parte serão informados ao Secretário-Geral do Conselho da Europa tão logo assinado ou depositado os instrumentos de ratificação, aceitação, aprovação ou adesão. O sigilo do pedido pode ser solicitado à Parte requerida. Se não for possível atender a essa solicitação, a Parte requerente será informada prontamente.

Nas hipóteses em que os pedidos de assistência mútua forem considerados urgentes, eles poderão ser enviados diretamente pelas autoridades judiciais da Parte requerente para autoridades similares da Parte requerida, devendo ser encaminhada cópia do pedido à autoridade central da Parte requerida por meio de sua congênere da outra parte. Quando não importar no cumprimento de medidas coercitivas, os pedidos ou as comunicações poderão ser realizados diretamente entre as autoridades competentes de cada Parte.

A Parte requerida pode condicionar a execução de um pedido de assistência à manutenção de sigilo, assim como poderá restringir a utilização do resultado do pedido à finalidade expressamente indicada pela Parte requerente, tal como apresentada em sua solicitação de assistência.

A conservação expedita de dados armazenados em computador (artigo 29) permite que a Parte requerente peça a imediata conservação de dados armazenados em um sistema de computador localizado no território da outra Parte, com o objetivo de, posteriormente, formular pedido de assistência mútua para busca ou acesso, apreensão ou guarda, ou revelação dos dados conservados.

O pedido de assistência deve: especificar a autoridade que requer a conservação; informar qual é o delito em apuração ou objeto de persecução e uma breve exposição dos fatos; indicar quais são os dados de computador a serem armazenados; dar informações a respeito do detentor dos dados de computador ou da localização do sistema de computador; declarar a necessidade da conservação; e manifestar a pretensão de formular futuro pedido de assistência mútua para busca ou acesso, apreensão ou guarda, ou revelação dos dados armazenados em computador.

O atendimento ao pedido de conservação de dados não exige a dupla incriminação e só pode ser recusado quando se referir a delito político ou conexo ou a Parte requerida

entender que a execução do pedido pode prejudicar a sua soberania, a segurança, a ordem pública ou outros interesses essenciais. O prazo para a conservação dos dados é de, no mínimo, sessenta dias, a fim de permitir que a Parte requerente apresente o pedido posterior de busca, acesso, apreensão, guarda ou revelação de dados, assim permanecendo até ser proferida a decisão final no último pedido.

Se a Parte requerida descobrir que há um provedor de serviço sediado em outro Estado envolvido na transmissão da comunicação, ela deverá entregar rapidamente os dados de tráfego à Parte requerente, de modo a identificar o provedor de serviço e o caminho pelo qual se deu a comunicação. A revelação de dados de tráfego só será recusada se a execução do pedido prejudicar a sua soberania, a segurança, a ordem pública ou outros interesses essenciais.

Os dados armazenados em um sistema de computador localizado no território de uma Parte poderão ser objeto de busca, acesso, apreensão, aguarda ou revelação que venham a ser pleiteadas por outra Parte para fins de investigação ou de persecução penal. Nesse caso, a colaboração se dará por meio da aplicação de instrumentos internacionais, de ajustes firmados com base em legislação uniforme ou de reciprocidade, todos diversos da Convenção de Budapeste, podendo haver resposta rápida quando os dados estiverem especialmente vulneráveis a perda ou a modificação, ou quando houver disposição diferente no tocante à cooperação expedita.

A dupla tipicidade somente será motivo de recusa do pedido de assistência quando ele for referente a delitos diferentes daqueles definidos dos artigos 2 a 11 da Convenção de Budapeste. Em relação aos crimes descritos na norma convencional, a exigência de dupla tipicidade se torna desnecessária na medida em que, ao subscreverem ou aderirem à convenção, as Partes se comprometem a adotar medidas legislativas para tipificar como crime as condutas descritas nos mencionados dispositivos.

Os dados de tráfego relacionados a determinada comunicação realizada por meio de computador e transmitida no território de uma das Partes também poderão ser objeto de interceptação em tempo real, em um contexto de assistência mútua. Nesse caso, as

condições e o procedimento aplicável serão ditados pela legislação interna para o cumprimento da medida.

A interceptação ou gravação, em tempo real, do conteúdo de comunicações transmitidas por um sistema de comunicações será tratada na forma dos acordos celebrados entre as Partes e das respectivas legislações internas. Nesse caso, a assistência mútua se dará por meio da aplicação de convenções internacionais, de ajustes firmados com base em legislação uniforme ou de instrumentos de reciprocidade, diversos da Convenção de Budapeste.

Embora tenha previsto procedimento para o acesso ao conteúdo de comunicações transmitidas por um sistema de computador, a Convenção de Budapeste estabeleceu que esse acesso, quando pleiteado por alguma Parte diferente daquela onde eles estejam armazenados, se dará segundo disciplinarem os tratados internacionais aplicáveis e a legislação doméstica da Parte requerida.

O texto convencional autoriza que as informações hauridas por uma Parte sejam reveladas e transmitidas *ex officio* a outra Parte desde que elas sejam capazes de auxiliar uma investigação ou procedimento levados a termo para a apuração de crimes tipificados pelo texto convencional, dentro das limitações da legislação interna da Parte que as detêm.

A hipótese prevista no artigo 32 da Convenção de Budapeste permite que uma Parte acesse, independentemente de sua localização, os dados públicos de um computador ou desde que o acesso tenha sido consentido, de forma legítima e voluntária, pela pessoa dotada de autoridade legal sobre eles.

O sistema de plantão disponível vinte e quatro horas por dia, nos sete dias da semana, permite que o órgão de contato indicado pela Parte preste assistência imediata para investigações ou procedimentos relacionados às infrações penais definidas na Convenção, bem como auxilie na obtenção de provas eletrônicas de crimes de outra natureza. Se houver permissão da legislação interna, poderá ser prestado diretamente o suporte técnico solicitado pela outra Parte e, do mesmo modo, a conservação de dados, a coleta de provas, o fornecimento de informação jurídica e a localização de suspeitos.

A fragilidade da Convenção, decorrente do brutal desenvolvimento tecnológico desde a data de sua criação, estava a impor a reavaliação dos mecanismos de assistência mútua. Como observa Rui Soares Pereira, essa evidente constatação resultou "no quadro das conclusões a que chegou o *Transborder Group* em 2014 tendo em vista o desenvolvimento de um instrumento jurídico (um novo Protocolo Adicional à Convenção sobre o Cibercrime) que regulasse o acesso transfronteiriço a dados"[18], fato que se tornou realidade com a adoção do Segundo Protocolo Adicional à Convenção de Budapeste, publicada em Bruxelas em 29 de março de 2022[19].

Assim, com o objetivo de reforçar a cooperação em matéria de cibercriminalidade, a obtenção de provas em formato eletrônico e possibilitar métodos de auxílio mútuo mais eficientes, sobretudo em situações de emergência, o Segundo Protocolo Adicional estabeleceu novos instrumentos procedimentais para cumprir tais finalidades. Além disso, a nova norma internacional trouxe regras mais claras a respeito da privacidade e da proteção de dados, temas tratados com alguma superficialidade na Convenção de Budapeste.

A grande inovação prevista no Segundo Protocolo Adicional são os procedimentos previstos em sua Seção 2 de cooperação direta entre prestadores de serviços situados em determinado território e as autoridades de outros países para a obtenção de dados necessários para uma investigação ou um procedimento penal. Segundo dispõe o texto adicional, as autoridades de determinado país podem apresentar pedidos de informação sobre o titular de um nome de domínio ou emitir uma injunção para obter dados específicos relativos a assinantes diretamente aos prestadores desses serviços estabelecidos em outro território.

---

[18] PEREIRA, Rui Soares. O acesso (unilateral e sem recurso a mecanismos de cooperação judiciária internacional) a dados armazenados em sistemas informáticas localizados no estrangeiro. In Revista de Estudios Europeos nº extraordinário monográfico, 1-2019, pág. 258. https://www.academia.edu/38946518/_O_acesso_unilateral_e_sem_recurso_a_mecanismos_de_coopera%C3%A7%C3%A3o_judici%C3%A1ria_internacional_a_dados_armazenados_em_sistemas_inform%C3%A1ticos_localizados_no_estrangeiro_in_Revista_de_Estudios_Europeos_I_2019_pp_246_273 acesso 27/09/2022.

[19] https://op.europa.eu/en/publication-detail/-/publication/8c7bad55-af76-11ec-83e1-01aa75ed71a1/language-pt/format-PDF/source-search acesso em 03 de outubro de 2022.

Quando se trata de informações sobre o nome do titular de um domínio (artigo 6º), a autoridade de determinado país solicita diretamente essa identificação à entidade que preste tal serviço sem precisar de qualquer ação das autoridades locais. Se o pedido não for atendido pelo prestador de serviço, devem ser indicadas as razões da recusa, sendo facultado à autoridade solicitante pleitear o concurso da autoridade daquele território para que essa última determine o cumprimento das medidas disponíveis para obter as informações.

Os dados específicos relativos a um assinante de serviço também podem ser solicitados por uma autoridade competente de determinado país mediante uma injução apresentada diretamente ao prestador de serviços localizado em outro território (artigo 7º).

O país onde estiver sediado o prestador de serviço poderá ressalvar que essa injunção só deverá ser atendida se suas autoridades também forem notificadas da injunção simultaneamente ou exigir que ela seja subscrita ou supervisionada por um procurador ou por uma autoridade judiciária. A autoridade local também poderá determinar que a prestadora de serviços somente informe os dados mediante o cumprimento de determinadas circunstâncias ou mesmo vedar o fornecimento dos dados solicitados na injunção.

Na hipótese de o prestador de serviços se recusar a fornecer os dados do assinante ou não os informar no prazo estabelecido, as autoridades da Parte emissora poderão se dirigir à autoridade competente do outro território, mediante a apresentação de injunção, para obrigar a apresentação das informações relativas a assinantes (7º artigo item 7).

Quando determinada Parte pretender a obtenção de dados de tráfego armazenados por um prestador de serviços localizado em outro território, ela deverá se dirigir às autoridades competentes locais para dar início à execução de uma injunção. A medida é prevista no artigo 8º do Segundo Protocolo, no qual foram enumerados os requisitos e relacionadas as condições necessárias ao atendimento do pedido. Uma vez preenchidas essas exigências, a autoridade competente local ordena a transmissão das informações e dos dados pretendidos para a Parte solicitante, sem demora injustificada.

O artigo 9º do Segundo Protocolo prevê a comunicação imediata de dados informáticos especificados e armazenados, em casos emergenciais, mediante o acionamento do ponto de contato previsto no artigo 35 da Convenção sobre Crime Cibernético. As situações de emergência são aquelas onde há um risco significativo e iminente para a vida ou para a segurança de um indivíduo, segundo prescreve o artigo 3º, item 2, letra c da norma complementar à Convenção.

O dispositivo comentado não explicitou se os dados informáticos pleiteados são os alusivos aos assinantes, aos dados de tráfego ou aos de conteúdo. Contudo, conforme esclareceu o Relatório Explicativo do Segundo Protocolo Adicional[20], a utilização da expressão "dados informáticos especificados e armazenados" pelo texto adicional objetivou dar a maior amplitude ao dispositivo de mútua assistência, reconhecendo a importância de se ter rápido acesso ao conteúdo dos dados armazenados, assim como aos dados de tráfego, quando estiver presente a hipótese prevista em seu artigo 3, item 2, letra c.

O auxílio mútuo pode ser solicitado de forma expedita em situações emergenciais, na forma estabelecida pelo artigo 10 do Segundo Protocolo Adicional. As atividades de auxílio mútuo abrangidas por essa espécie de procedimento célere são diversas daquelas atendidas pelo artigo 9º da norma e se submetem ao procedimento descrito no texto.

A norma também prescreve como pleitear a tomada de depoimentos e declarações de testemunhas e de peritos mediante videoconferência, tal como se vê em seu artigo 11º. Por fim, é possível a criação de equipes de investigação conjunta, com o objetivo de facilitar investigações ou procedimentos penais.

No campo da proteção aos dados pessoais, o Segundo Protocolo Adicional avançou bem mais do que a norma supranacional por ele complementada. O artigo 14º estabelece o âmbito de aplicação do protocolo quanto ao tratamento dos dados recebidos, a finalidade e a utilização das informações prestadas, a obrigatoriedade para assegurar a qualidade e a integridade dos dados pessoais.

---

[20] CONSELHO DA UNIÃO EUROPEIA. Treaty Series nº 224 item 155 chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://rm.coe.int/1680a49c9d

Além disso, o dispositivo define quais são os dados sensíveis que merecem salvaguardas e a necessidade de ser estabelecido um período de sua conservação, sujeito à revisão periódica. Há também a previsão de medidas para garantir a intervenção humana em decisões automatizadas, a imposição de medidas tecnológicas, físicas e associativas adequadas para a proteção de dados pessoais, bem como regras específicas sobre incidentes de segurança.

O artigo 14º do Segundo Protocolo Adicional assegura que a pessoa cujos dados pessoais tenham sido transmitidos mediante os instrumentos nele previstos tenha o direito de receber uma cópia da documentação conservada sobre ela, podendo ser levantadas restrições a esse direito quando se fizer necessária a proteção de interesses de terceiros ou quando presentes objetivos importantes de interesse público.

Na hipótese de os dados pessoais armazenados forem inexatos ou submetidos a tratamento incorreto, a pessoa atingida pode pleitear a sua retificação. Caso esses direitos lhe tenham sido negados, a Segundo Protocolo Adicional assegura a utilização de recursos judiciais ou extrajudiciais para debelar a violação.

A transferência de dados pessoais pode ser suspensa quando presentes provas substanciais de que a Parte solicitante viola sistematicamente e de forma grave as disposições sobre a proteção de dados pessoais ou quando é iminente essa violação.

Embora seja muito recente, o Segundo Protocolo Adicional tem recebido críticas por parte de entidades preocupadas com a proteção de dados pessoais, assim como de doutrinadores mais atentos ao alcance das medidas de reforço de investigações e de persecução penal para acessar os dados de computador armazenados no exterior.

Alguns setores da sociedade civil internacional censuraram a ausência de participação de especialistas, a falta de transparência das discussões e a excessiva celeridade do grupo criado pelo Comitê Europeu para estudar a adoção de novas medidas de reforço para a Convenção de Budapeste, como assinala Bruna Martins dos Santos[21].

[21] SANTOS, Bruna Martins dos. Budapest Convention on Cybercrime in Latin America: a brief analysis of adherence and implementations in Argentina, Brazil, Chile, Colombia and Mexico. https://www.derechosdigitales.org/wp-content/uploads/ENG-Ciberdelincuencia-2022.pdf Acesso em 23/10/2022

De igual modo, são muito válidas as observações de Veridiana Alimonti[22]ao destacar a ausência da obrigatoriedade de supervisão judicial sobre as solicitações de acesso transfronteiriço aos dados cadastrais de assinantes e aos dados de tráfego guardados em outro país.

No seu modo de ver, ao não ser exigida a participação judicial como procedimento padrão no pedido de injunção e sim como mero objeto de ressalva, na forma do artigo 7º, parágrafo 2, letra b do Segundo Protocolo Adicional, o sistema de proteção de dados resta vulnerabilizado, por autorizar um acesso mais permissivo aos dados armazenados.

Por outro lado, são relevantes as anotações de Halefom H. Abraha[23] quanto ao acesso transfronteiriço de dados previsto na Convenção de Budapeste, mesmo com as disposições alargadas previstas no Segundo Protocolo Adicional. Segundo o doutrinador, as medidas propostas nos dois estatutos se limitam à obtenção de categorias específicas de dados, como as informações sobre os assinantes ou relacionadas aos dados de tráfego. Os procedimentos para o acesso aos dados de conteúdo armazenados foram relegados aos tratados e instrumentos de mútua colaboração, frequentemente criticados por sua morosidade.

Após discorrer sobre as diversas abordagens do problema do acesso transfronteiriço a dados informatizados (reformista, unilateralista, internacionalista e diferenciada) e enfatizar a inexistência de um sistema que resolva todas as questões incidentes, Halefom H. Abraha entende que “a abordagem diferenciada oferece uma opção relativamente realista para lidar com o problema jurisdicional e de conflitos de lei da nuvem por meio de acordos bilaterais de compartilhamento de dados baseados no

---

[22] ALIMONTI, Veridiana. “Assessing New Protocol to the Cybercrime Convention in Latin America: Concerns, Human Rights Considerations, and Mitigation Strategies” is released under a Creative Commons Attribution 4.0 International License (CC BY 4.0). Electronic Frontier Foundation, 2022 Chrome extension://efaidnbmnnnibpcajpcglclefindmkaj/https://necessaryandproportionate.org/files/protocol-cybercrime-convention-latam.pdf Acesso em 30 de setembro de 2022

[23] ABRAHA, Halefom H. Law enforcement access to electronic evidence across borders: mapping policy approaches and emerging reform initiatives. International Journal of Law and Information Technology, Volume29, Issue 2, Summer 2021, Pages 118–153. https://academic.oup.com/ijlit/article/29/2/118/6224386 Acesso 03 de outubro de 2022.

princípio da reciprocidade e um compromisso compartilhado com o estado de direito e a proteção da privacidade"[24].

A base dessa nova geração de acordos internacionais é o *Clarifying Lawful Overseas Use of Data Act,* convenientemente abreviado como *CLOUD Act,* legislação promulgada pelos Estados Unidos da América em março de 2018[25]. Assim, após ser assinado o acordo entre os EUA e a sua contraparte:

> o governo estrangeiro qualificado poderá ordenar a produção de qualquer tipo de dados, incluindo dados de conteúdo (como conteúdo de e-mail e mensagens de texto) diretamente de provedores de serviços baseados nos EUA sem passar pelo processo de MLA. Ao remover os estatutos de bloqueio nos EUA e nos países parceiros estrangeiros, os acordos bilaterais previstos pelo *CLOUD Act* evitariam potenciais obrigações legais conflitantes.[26]

Evidentemente, não se trata de uma fórmula perfeita e infensa a críticas, sobretudo ante a impossibilidade de se alcançar uma escala global, tendo em vista a diferença de valores existente entre diversos países e os Estados Unidos da América, inclusive no campo da proteção de dados, fator que inviabiliza a celebração de muitos acordos bilaterais.

No entanto, uma vez celebrado o acordo, as autoridades do país solicitante terão acesso rápido aos dados e a seus conteúdos, mediante solicitação direta às empresas que os armazenam.

Embora tenha sido aprovada pelo Poder Legislativo brasileiro no final de 2021, a Convenção de Budapeste aguarda a ratificação pela Presidência da República. O Segundo Protocolo Adicional daquele estatuto internacional ainda não foi assinado pelo Brasil.

Por outro lado, o Anteprojeto de Lei de Proteção de Dados para a segurança pública e persecução penal, mais conhecido como a LGPD Penal, também não evolui no Parlamento, apesar da premência e da importância que o tema merece, gerando o enfraquecimento do sistema brasileiro de proteção de dados.

Como vimos anteriormente, as medidas legislativas preconizadas pela Convenção de Budapeste e de seu Segundo Protocolo Adicional não atritam com o ordenamento

---

[24] ABRAHA, Halefom H. Op. cit. pág 19. Texto vertido para o português com recurso Google.

[25] ESTADOS UNIDOS DA AMÉRICA. S.2383/H.R. 4943. The Clarifying Overseas Use of Data (CLOUD ACT). 2018. Disponível em: https://www.congress.gov/115/bills/hr4943/BILLS-115hr4943ih.pdf Acesso em: 10 de outubro de 2022.

[26] ABRAHA, Halefom H. Op. cit. pág 21. Texto vertido para o português com recurso Google

jurídico nacional. Os tipos penais nela contemplados já se encontram tipificados em nossa legislação doméstica, assim como as medidas cautelares e as fórmulas procedimentais descritos no diploma internacional encontram muito paralelismo com as vigentes no Brasil.

O mesmo pode ser dito em relação às regras atinentes à extradição previstas na Convenção de Budapeste, pois, no que é relevante, são coincidentes em grande parte com os dispositivos constantes da Lei de Migração, de nº 13.445/2017.

De todo modo, a legislação brasileira que trata do acesso às evidências informáticas é composta pela Constituição da República, pela Lei das Interceptações Telefônicas e pelo Marco Civil da Internet.

O inciso XII do artigo 5º da Constituição da República assegurou o sigilo da correspondência e das comunicações telegráficas, mas ressalvou o afastamento dessa garantia nos casos das comunicações de dados e telefônicas, desde que autorizado por ordem judicial, na forma da lei e para fins de investigação criminal ou instrução processual penal.

A Lei 9.296/96 regulamentou o dispositivo constitucional e possibilitou a interceptação do fluxo de comunicações em sistemas de informática e telemática, desde que realizada em condições excepcionalíssimas[27], o que tornou esse meio de prova merecedor do maior grau de proteção do ordenamento jurídico brasileiro, "assim considerada a comunicação de dados entre dois dispositivos ou sistemas computacionais"[28].

Os registros de conexão, definidos nos incisos VI, VII e VIII do artigo 5º do Marco Civil da Internet[29], também denominados como metadados ou dados de tráfego, são

[27]BRASIL. Lei 9.296/96: Art. 2° Não será admitida a interceptação de comunicações telefônicas quando ocorrer qualquer das seguintes hipóteses:
I - não houver indícios razoáveis da autoria ou participação em infração penal;
II - a prova puder ser feita por outros meios disponíveis;
III - o fato investigado constituir infração penal punida, no máximo, com pena de detenção.

[28] MOURA, Maria Tereza Rocha de Assis. BARBOSA, Daniel Marchionatti. Dados digitais: interceptação, busca e apreensão e requisição. In Direito, processo e tecnologia. Wolkart, Erik Navarro; Laux, Francisco de Mesquita; Ravagnani, Giovani dos Santos; Lucon, Paulo Henrique dos Santos (org.). Edição do Kindle

[29] BRASIL. Lei 12.965/14. Art. 5°:

"indissociáveis de comunicações e de outras atividades concretas dos usuários na rede, considera-se que os metadados integram a intimidade, ficando o afastamento de seus sigilos condicionado à cláusula de reserva de jurisdição, como consignado expressamente no texto legal (art. 13, § 5° e art. 15, § 3°)"[30].

Entretanto, em se tratando de metadados, os requisitos que autorizam a ordem judicial de acesso são bem mais tênues daqueles impostos à interceptação do fluxo de comunicações em sistemas de informática.

Esses tratamentos díspares ficam mais acentuados quando se observa que a lei não prescreveu qualquer limitação temporal para o acesso aos dados já armazenados em sistemas de informática, permitindo o acesso irrestrito a todo o conteúdo existente no sistema ou no equipamento apreendido. Como observa Carina Quito, "enquanto em tráfego, as mensagens trocadas são protegidas com rigor; no instante seguinte ao seu armazenamento – momento esse que sequer pode ser precisado –, o rigor desaparece, viabilizando acesso praticamente irrestrito aos registros de conteúdos comunicados, desde que haja, para tanto, autorização judicial"[31].

O acesso aos dados cadastrais de assinantes não resta sempre condicionado à prévia ordem judicial, na medida em que o § 3º do artigo 10 da Lei 12.965/14 permite que as autoridades administrativas possam requisitá-los, desde que detenham a competência legal para tanto e nas hipóteses previstas em lei para a investigação de certos delitos que, por sua gravidade, exigem maior grau de eficiência em sua persecução.

Deste modo, postas balizas do ordenamento jurídico em vigor no Brasil, percebemos que a regra geral para o acesso aos dados cadastrais, aos metadados, aos

---

VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;
VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e
VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

[30] QUITO, Carina. As quebras de sigilo telemático no processo penal e o paradoxo do acesso irrestrito à comunicações armazenadas. In Direito, processo e tecnologia. Wolkart, Erik Navarro; Laux, Francisco de Mesquita; Ravagnani, Giovani dos Santos; Lucon, Paulo Henrique dos Santos (org.). Edição do Kindle

[31] QUITO, Carina. Op. cit. Edição do Kindle

dados de conteúdo e à interceptação de comunicações informáticas é a da reserva de jurisdição.

Essa conclusão tem uma consequência indelével: os procedimentos de assistência mútua contidos na Convenção de Budapeste e em seu Segundo Protocolo Adicional deverão observar absoluto paralelismo entre suas disposições e as cláusulas equivalentes previstas em nossa legislação.

Deste modo, haverá autorização judicial, seja o Brasil parte requerente ou requerida, quando se tratar de: revelação de dados de tráfego (artigo 30 da Convenção de Budapeste); acesso a dados de computador armazenados (artigo 31 da Convenção de Budapeste); interceptação de dados de tráfego em tempo real (artigo 33 da Convenção de Budapeste); interceptação do conteúdo das comunicações (artigo 34 da Convenção de Budapeste).

De forma igual, incidirá a reserva de jurisdição nas hipóteses de: emissão de injunção para obtenção de dados de tráfego ou ante a recusa do prestador de serviço de informar tais dados específicos relativos a assinantes (artigo 8º do Segundo Protocolo Adicional); e pedido de assistência para obtenção expedita de dados especificados e armazenados em caso de emergência (artigo 9º do Segundo Protocolo Adicional).

A conservação expedita de dados armazenados em computador, prevista nos artigos 16 e 29 da Convenção guardam semelhanças com a medida preconizada no § 2º do artigo 13 do Marco Civil da Internet, pois ambas constituem atividades cautelares cujo objetivo comum é a preservação de dados armazenados, inclusive os de tráfego.

Na hipótese prevista pela legislação brasileira, tanto a autoridade policial, a administrativa, quanto o Ministério Público podem requerer cautelarmente o alargamento do prazo de guarda dos dados. Assim, o pedido de assistência mútua visando a conservação expedita de dados à legislação brasileira, prevista no artigo 29 da Convenção de Budapeste, poderá ser formulada por uma autoridade policial ou por membro do *Parquet* de outra Parte, desde que esteja relacionada a investigação ou a procedimento criminal.

Por óbvio, o acesso transfronteiriço a dados em um computador mediante consentimento do titular ou por via de sistema de acesso público, também dispensam autorização judicial (artigo 32 da Convenção de Budapeste). Do mesmo modo, a realização de videoconferência para oitiva de testemunhas ou de peritos tampouco necessita da ação de uma autoridade judiciária, o mesmo ocorrendo no tocante à formação de equipes de investigação conjuntas, salvo se houver a hipótese de medida cautelar sujeita à reserva de jurisdição.

Em outra medida, o Segundo Protocolo Adicional permite que uma autoridade, policial ou judiciária, tenha acesso direto a entidade que preste serviços de registro de nomes de domínio para que seja identificado ou contactado o titular do respectivo domínio, na forma do artigo 6º do Segundo Protocolo Adicional.

O mesmo modo de proceder pode ser adotado para a obtenção de dados específicos relativos aos assinantes armazenados por um prestador de serviços, desde que cumpridos os requisitos descritos no artigo 7º do Segundo Protocolo Adicional. O Marco Civil da Internet contém dispositivo muito semelhante quando excepciona a regra geral da reserva de jurisdição para autorizar "o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição."[32]

Não obstante os avanços dos instrumentos colocados à disposição das Partes para acessar determinados dados armazenados no exterior, merece ser registrado que a Convenção de Budapeste e, da mesma forma, o Segundo Protocolo Adicional, em regra, não trataram do acesso direto ao conteúdo das mensagens já armazenadas. Há a exceção das situações definidas como emergenciais (artigo 9° do Segundo Protocolo Adicional), quando é possível o acesso a todas as espécies de dados, mediante a utilização dos pontos de contato da rede 24/7 referida no artigo 35 da Convenção de Budapeste.

As normas supranacionais aqui comentadas tampouco são aplicáveis à interceptação ou à gravação ao conteúdo de comunicações específicas transmitidas por

[32] BRASIL, Lei nº 12.965/2014. Artigo 10 § 3º.

meio de um sistema de computador. Essas atividades, segundo prescreve o artigo 23 da Convenção de Budapeste, devem ser implementadas mediante a cooperação mútua, na forma do disposto em seu Capítulo III, e por meio:

> da aplicação de instrumentos internacionais pertinentes de cooperação internacional em assuntos penais, de ajustes firmados com base em legislação uniforme ou de reciprocidade, e da legislação doméstica, o mais possível, para a realização das investigações ou procedimentos acerca de crimes de computador, ou para a coleta de provas eletrônicas desses crimes[33]

Deste modo, quando não ocorrentes situações de emergência, os instrumentos necessários para a obtenção desses dados de conteúdo ainda são as cartas rogatórias, os acordos mútuos de colaboração, a legislação uniforme e a reciprocidade, pois, como assinala Bruna Veríssimo Lima Santos, ainda "haverá necessidade não apenas de instrumentos jurídicos, como acordos bilaterais e multilaterais mais abrangentes, mas também do reforço na capacitação dos agentes públicos a fim de que estejam preparados para manejar esses novos mecanismos."[34]

No mesmo sentido é a manifestação de Carlos Affonso Souza e de Christian Perrone quando admitem ser mais prudente "concluir a adesão do Brasil à Convenção de Budapeste e, a partir dela, progressivamente ampliar as facilidades para acesso a dados localizados no exterior via mecanismos de cooperação internacional"[35], do que introduzir nova legislação que acirra uma queda de braços jurisdicional entre dois países soberanos.

Conforme foi acentuado anteriormente, o acordo executivo bilateral celebrado sob os auspícios do *Cloud Act* é o que permite o acesso mais amplo aos bancos de dados situados nos Estados Unidos da América, pois, uma vez celebrado o acordo, o governo estrangeiro pode ter acesso direto ao conteúdo de comunicações eletrônicas armazenadas por provedores de serviço naquele país e vice-versa. Segundo a legislação norte-americana, para que um governo estrangeiro seja elegível para celebrar esse acordo

---

[33] CONSELHO DA EUROPA. Convenção sobre o Crime Cibernético. Art. 23.

[34] SANTOS, Bruna Veríssimo Lima. Adoção da Convenção de Budapeste pelo Brasil: desafios e perspectivas. In Proteção de dados e tecnologia, estudos da pós-graduação em direito digital. BRANCO, Sérgio; TEFFÉ, Chiara de (Coords.). Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; ITS/Obliq, 2022. Pág. 283

[35] SOUZA, Carlos Affonso; PERRONE, Christian. 'Fake news' e acesso a dados armazenados no exterior. https://www.jota.info/coberturas-especiais/liberdade-de-expressao/fake-news-e-acesso-a-dados-armazenados-no-exterior-30062020 acesso 15/09/2022

executivo é necessário que comprove que suas normas domésticas asseguram proteções robustas de privacidade e de liberdades civis, critério que pode ser demonstrado pelo fato de ser signatário da Convenção de Budapeste.

Portanto, não obstante as limitações ao acesso ao conteúdo de comunicações transmitidas por um dispositivo informático, é extremamente válida a assinatura da Convenção de Budapeste pelo Brasil, sobretudo pelo fato de essa adesão servir "como porta de entrada para qualquer futura negociação de novos acordos bilaterais, seja no marco do Cloud Act norte-americano, seja no *e-Evidence Project* da União Europeia"[36].

4. Conclusão.

Depois de quase dois decênios, finalmente o Brasil aderiu à Convenção de Budapeste. A entrada do país nesse grupo de nações constitui importante passo para o aprimoramento da persecução penal dos crimes do computador, sobretudo no campo da cooperação internacional.

No concernente ao Direito Penal, as sugestões de tipificação de condutas contidas no instrumento internacional não representaram a inserção de qualquer nova figura típica em nosso ordenamento, posto que os delitos nele definidos já estão contemplados na legislação nacional.

Apesar disso, se faz necessária a ressalva de que a reserva legal já constituída no país, assim como qualquer outra que venha a ser estabelecida de maneira mais ampla para o indivíduo, deve se sobrepor às indicadas. Isto se dá pelo respeito irrestrito às garantias fundamentais construídas pelo nosso processo constitucional interno, apesar de nosso espírito cooperativo junto à comunidade internacional.

No tocante aos dispositivos processuais indicados na Convenção de Budapeste, em sua grande parte, eles estão em consonância com a Constituição da República, com a exceção de algumas ressalvas pontuais destacadas neste parecer, especialmente no

[36] SOUZA, Carlos Affonso; PERRONE, Christian. Op. cit. acesso 15/09/2022

tocante às medidas que impactam o direito de não fazer prova contra si próprio e que flexibilizam o cumprimento de mandados de busca e apreensão de dados armazenados em sistemas ou computadores que não constaram da ordem judicial primitiva.

Por outro lado, a Convenção explicita a necessidade de ordem judicial para varejar o conteúdo de dispositivos encontrados no curso de busca e apreensão domiciliar ou pessoal, algo que não está claramente normatizado em nosso país, embora a práxis forense revela que esse cuidado é observado pela grande maioria dos magistrados.

A maior influência exercida pela Convenção de Budapeste ocorre no segmento da cooperação internacional. As medidas preconizadas facilitam a obtenção de dados que muito contribuem para as investigações criminais e para as persecuções penais, garantindo a preservação de informações que poderão elucidar ou comprovar a prática de delitos. No entanto, o acesso ao conteúdo dos dados ainda está condicionado ao acionamento aos instrumentos de cooperação tradicionais, como os tratados de assistência mútua e as cartas rogatórias.

Na forma do Segundo Protocolo Adicional da Convenção de Budapeste, o varejamento expedito aos dados substanciais das comunicações eletrônicas só é possível em situações emergenciais nas quais exista perigo de risco significativo e eminente ao indivíduo, mediante o acionamento da autoridade central, a ser disponibilizada vinte quatro horas por dia nos sete dias da semana.

A adesão à Convenção de Budapeste traz também a consequência de habilitar o Brasil a firmar acordo bilateral com os Estados Unidos da América, sob a égide do *Cloud Act*, instrumento que permite às autoridades judiciais estrangeiras a requisição direta de dados, inclusive de conteúdo, dos provedores de armazenamento de dados estabelecidos naquele país. Com isso, estará viabilizado o objetivo de muitas autoridades judiciárias brasileiras de acessar o conteúdo de dados armazenados nos Estados Unidos da América, sem que submetam os escritórios de representação dessas empresas ao constrangimento das astreintes e, até, de ordem de prisão por desobediência de seus representantes.

Assim, o parecer ora ofertado concluiu que a maior parte dispositivos da Convenção de Budapeste foi recepcionada pela Constituição da República.

Deve ainda ser enfatizado que a indicação e a recomendação favorável com as ressalvas antes apontadas não se dão por uma pura análise jurídico-penal da Convenção de Budapeste, mas também pela importância que se dá para a compreensão de fenômenos internacionais dentro de um contexto de mundo globalizado como um espaço de constante disputa pela hegemonia, controle e participação em diferentes mercados, valendo-se de delimitações políticas, geográficas, culturais, econômicas e, também, jurídicas.

A aprovação da Convenção de Budapeste, tal como aqui sugerida, não reflete uma posição técnica divorciada da realidade, tampouco um desejo néscio de fazer parte qualquer grupo econômico, mas sim de uma maneira de avaliar as indicações que são feitas em nossa Comissão com sua intrínseca complexidade.

Compreendemos, assim, que além das ressalvas eminentemente jurídicas, esta aprovação da Convenção se dá na perspectiva crítica de inserir o país dentro de blocos internacionais, mas sem deixar de compreender a legislação penal como mais um dos instrumentos jurídico-políticos que compõem o ecossistema de instrumentos daquela disputa.

Rio de Janeiro, 07 de dezembro de 2022

RENATO TONINI ANDRÉ NASCIMENTO FERNANDO HENRIQUE CARDOSO NEVES

RELATORES

Referências

ABRAHA, Halefom H. Law enforcement access to electronic evidence across borders: mapping policy approaches and emerging reform initiatives. International Journal of Law and Information Technology, Volume29, Issue 2, Summer 2021. https://academic.oup.com/ijlit/article/29/2/118/6224386 Acesso em 03 de outubro de 2022.

ALIMONTI, Veridiana. "Assessing New Protocol to the Cybercrime Convention in Latin America: Concerns, Human Rights Considerations, and Mitigation Strategies" is released under a Creative Commons Attribution 4.0 International License (CC BY 4.0). Electronic Frontier Foundation, 2022 Chrome extension://efaidnbmnnnibpcajpcglclefindmkaj/https://necessaryandproportionate.org/files/protocol-cybercrime-convention-latam.pdf Acesso em 30 de setembro de 2022

ARAÚJO, Nádia de. Direito internacional privado, teoria e prática brasileira. São Paulo: Editora Revista dos Tribunais: 2020.

BRASIL. CÂMARA DOS DEPUTADOS. Anteprojeto de Lei de Proteção de Dados para a segurança pública e persecução penal. Acesso em 30 de setembro de 2022. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristas-dados-pessoais-seguranca-publica/documentos/outros-documentos/DADOSLGPD comissaoprotecaodadossegurancapersecucaoFINAL.pdf

BRASIL. Lei 9.296/96

BRASIL. Lei 12.965/14

BRASIL. SENADO FEDERAL Decreto legislativo 37/2021. Acesso em 23 de agosto de 2022 https://legis.senado.leg.br/norma/35289207/publicacao/35300588

BRASIL SENADO FEDERAL. PDL 255/2021 Acesso em 02 de março de 2022 https://legis.senado.leg.br/sdleg-getter/documento?dm=9026819&ts=1656678500768&disposition=inline

BRASIL, Supremo Tribunal Federal, Tribunal Pleno, RE 418.416, rel. Min. Sepúlveda Pertence, j. 10.mai.06, DJ 19.dez.06.

BRASIL. Supremo Tribunal Federal, Pleno, RE 971.959, rel. Min. Luiz Fux, j. 14.nov.18, DJe 31.jul.20.

CURVELO, Erick Vieira. Ódio, liberdade e censura: quando o Supremo entra na sala. Artigo Aceito para publicação Direito Digital e Setor Público. 2020.2 Pós-graduação em Direito Digital. CEPED UERJ ITS.

CONSELHO DA UNIÃO EUROPEIA. Segundo protocol adicional à Convenção sobre crimes cibernéticos. Acesso em 29 de março de 2022. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://data.consilium.europa.eu/doc/document/ST-14898-2021-INIT/pt/pdf

CONSELHO DA UNIÃO EUROPEIA TREATY SERIES – No. 224 Explanatory Report to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence

chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://rm.coe.int/1680a49c9d

D´AVILA, Fabio Roberto; SANTOS, Daniel Leonhardt. Direito Penal e criminalidade informática. Breves aproximações dogmáticas. In Revista Due In Altum Cadernos de Direito, vol. 8, nº 15, mai-ago 2016.

EILBERG, Daniela Dora et alia. Os cuidados com a Convenção de Budapeste. https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/os-cuidados-com-a-convencao-de-budapeste-08072021

ESTADOS UNIDOS DA AMÉRICA. S.2383/H.R. 4943. The Clarifying Overseas Use of Data (CLOUD ACT). 2018. Disponível em: https://www.congress.gov/115/bills/hr4943/BILLS-115hr4943ih.pdf Acesso em: 10 de outubro de 2022.

FERNANDES, Antonio Scarance; ALMEIDA, José Raul Gavião de; MORAES, Maurício Zanoide de (orgs.). Sigilo no Processo Penal – Eficiência e Garantismo. S.Paulo, 2008, ed. RT

HADDAD, Carlos Henrique Borlido. Conteúdo e Contornos do Princípio contra a Auto-Incriminação, Campinas, 2005, Bookseller, p. 217;

JESUS, Damásio de; MILAGRE, José Antonio. Marco civil da internet: comentários à Lei 12.965, de 23 de abril de 2014. São Paulo: Saraiva, 2014.

LAUX, Francisco de Mesquita. Limites da jurisdição no âmbito da internet: análise da experiência francesa sob a perspectiva do caso Google Llc Vs. Commission Nationale de L´informatique e des Libertes (Cnil) – 399.922, Conseil D´état. In WOLKART, Erick Navarro Wolkart et. alia (coordenador). Direito, processo e tecnologia. 1 ed. – São Paulo: Thomson Reuters Brasil, 2020.

LAUX, Francisco de Mesquita. Redes sociais e limites da jurisdição: plano da territorialidade e efetividade. São Paulo: Thomson Reuters Brasil. 2021

MACHADO, André Augusto Mandes; KEHDI, Andre Pires de Andrade. *Sigilo das comunicações e de dados*. *In* FERNANDES, Antonio Scarance; ALMEIDA, José Raul Gavião de; MORAES, Maurício Zanoide de (orgs.). Sigilo no Processo Penal – Eficiência e Garantismo. S.Paulo, 2008, ed. RT, p. 243; e SIDI, Ricardo. A Interceptação das Comunicações Telemáticas no Processo Penal, B.Horizonte, 2016, Ed. D'Plácido

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. Curso de Direito Constitucional, S.Paulo, 2019, Saraiva Educação

MOURA, Maria Thereza Rocha de Assi; BARBOSA, Daniel Marchionatti. Dados digitais: interceptação, busca e apreensão e requisição. In WOLKART, Erick Navarro Wolkart et. alia (coordenador). Direito, processo e tecnologia. 1 ed. – São Paulo: Thomson Reuters Brasil, 2020.

NUNES, Duarte Rodrigues. Os meios de obtenção de prova previstos na Lei do Cibercrime. 2ª edição revista e atualizada. Coimbra: Gestlegal, 2021.

PEREIRA, Rui Soares. O acesso (unilateral e sem recurso a mecanismos de cooperação judiciária internacional) a dados armazenados em sistemas informáticas localizados no estrangeiro. In Revista de Estudios Europeos nº extraordinário monográfico, 1-2019.

https://www.academia.edu/38946518/_O_acesso_unilateral_e_sem_recurso_a_mecanismos_de_cooperação_judici%C3%A1ria_internacional_a_dados_armazenados_em_sistemas_inform%C3%A1ticos_localizados_no_estrangeiro_in_Revista_de_Estudios_Europeos_I_2019_pp_246_273 acesso 27/09/2022

PITOMBO, Cleunice Bastos. Da Busca e Apreensão no Processo Penal, S.Paulo, 2005, ed. RT;

QUEIJO, Maria Elizabeth. O Direito de Não Produzir Prova contra Si Mesmo, S.Paulo. 2003, Saraiva;

QUITO, Carina. As quebras de sigilo telemático no processo penal e o paradoxo do acesso irrestrito à comunicações armazenadas. In Direito, processo e tecnologia. Wolkart, Erik Navarro; Laux, Francisco de Mesquita; Ravagnani, Giovani dos Santos; Lucon, Paulo Henrique dos Santos (org.). Edição do Kindle.

RAMALHO, David Silva. A recolha de prova penal em sistema de computação em nuvem. In Revista de Direito Intelectual nº 2- 2014. Edições Almedina. Lisboa. Dezembro de 2014.

SARLET, Ingo Wolfgang; MARINONI, Luiz Guilherme; MITIDIERO, Daniel. Curso de Direito Constitucional, S.Paulo, 2018, Saraiva Educação

SANTOS, Bruna Martins dos. Budapest Convention on Cybercrime in Latin America: a brief analysis of adherence and implementations in Argentina, Brazil, Chile, Colombia and Mexico. https://www.derechosdigitales.org/wp-content/uploads/ENG-Ciberdelincuencia-2022.pdf Acesso em 23/10/2022

SANTOS, Bruna Veríssimo Lima. Adoção da Convenção de Budapeste pelo Brasil: desafios e perspectivas. *In* Proteção de dados e tecnologia, estudos da pós-graduação em direito digital. BRANCO, Sérgio; TEFFÉ, Chiara de (Coords.).Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio de Janeiro; ITS/Obliq, 2022.

SIDI, Ricardo. A Interceptação das Comunicações Telemáticas no Processo Penal, B.Horizonte, 2016, Ed. D'Plácido.

SOUZA, Carlos Affonso. STF deve reconhecer acordo para acesso a dados no exterior. https://www.jota.info/opiniao-e-analise/artigos/stf-deve-reconhecer-acordo-para-acesso-a-dados-no-exterior-13042021

SOUZA, Carlos Affonso; PERRONE, Christian. 'Fake news' e acesso a dados armazenados no exterior. https://www.jota.info/coberturas-especiais/liberdade-de-expressao/fake-news-e-acesso-a-dados-armazenados-no-exterior-30062020 acesso 15/09/2022

SOUZA, Gills Lopes Macêdo; PEREIRA, Dalliana Vilar. A Convenção de Budapeste e as lei brasileiras. Trabalho apresentado e aceito para publicação nos Anais do *1° Seminário Cibercrime e Cooperação Penal Internacional*, organizado pelo CCJ da UFPB e pela *Association Internacionale de Lutte Contra la Cybercriminalite* (França), João Pessoa/PB, maio de 2009.

STRECK, Lenio Luiz. As Interceptações Telefônicas e os Direitos Fundamentais, P.Alegre, 2001, Livr. do Advogado

SUPREMO TRIBUNAL FEDERAL. ADC nº 51, processo nº 0014496-52.2017.1.00.0000, Relator Ministro Gilmar Mendes.

SUPREMO TRIBUNAL FEDERAL, Pleno, RE 971.959, rel. Min. Luiz Fux, j. 14.nov.18, DJe 31.jul.20;

TÔRRES, Ana Maria Campos. A Busca e Apreensão e o Devido Processo Legal, Rio, 2004, Forense;

TUCCI, Rogério Lauria. Direitos e Garantias Individuais no Processo Penal Brasileiro, S.Paulo, 2004, Saraiva;

VIOLA, Mário. HERINGER, Leonardo. CARVALHO, Celina. O anteprojeto da LGPD penal e as regras sobre a transferência internacional de dados pessoais. Editoração e revisão Celina Botino e Christian Perrone. Great for Paternship. Instituto de Tecnologia & Sociedade do Rio. Agosto de 2021.