Aquisição de provas criminais eletrônicas no Brasil à luz da Convenção de Budapeste, do Cloud Act dos Estados Unidos da América e do Direito da União Europeia[1]

Acquisition of electronic criminal evidence in Brazil in the light of the Budapest Convention, the Cloud Act of the United States of America and European Union Law

WILSON ANTONIO PAESE SEGUNDO[2]
wpaese@gmail.com

GALILEU – REVISTA DE DIREITO E ECONOMIA · e-ISSN 2184-1845
Volume XXII · 1st January Janeiro – 31ST December Dezembro 2022 · pp. 63-79
DOI: https://doi.org/10.26619/2184-1845.XXIII.1/2.4
Submitted on September 2nd, 2022 · Accepted on September 21st, 2022
Submetido em 2 de Setembro, 2022 · Aceite a 21 de Setembro, 2022

RESUMO O escopo do trabalho, centrado na etapa oficial da investigação preliminar de crimes de competência do Brasil, busca verificar se, a obtenção de metadados e de conteúdo eletrônico diretamente com o ente privado que a armazena, encontra paralelo nas disposições da Convenção de Budapeste, na legislação pertinente da União Europeia e no Cloud Act dos Estados Unidos da América. O tema assume relevo atualmente, porquanto a autoria da maioria das infrações penais comuns somente pode ser descoberta e seus autores identificados, mediante a obtenção célere de provas eletrônicas, invariavelmente, armazenadas em território estrangeiro, ao passo que os tradicionais instrumentos de cooperação mútua são considerados obsoletos para lidar com o problema.

PALAVRAS-CHAVE investigação criminal; provas eletrônicas; dispensa do MLA; obtenção direta com o ente privado; Brasil e Direito comparado.

1 Este artigo corresponde ao trabalho apresentado na Unidade Curricular de «Teoria Geral do Direito Policial», ministrada pelo Professor Doutor Manuel Monteiro Guedes Valente, no âmbito do Mestrado em Direito – Ciências Jurídico-Policiais. O estudo foi desenvolvido no âmbito do Projeto de I&D: *Corpus Delicti* – Estudos de Criminalidade Organizada Transnacional, sediado no Ratio Legis – Centro de Investigação e Desenvolvimento em Ciências Jurídicas da Universidade Autónoma de Lisboa.

2 Delegado da Polícia Federal. Mestrabndo em Direito – Ci~encias Jurídico-Policiais da Universidade Autónoma de Lisboa. Invetsigador colaborador do Ratio Legis, projeto de I&D: Corpus Delicti – Estudos de Criminalidade Orgnaizada Transnacional.

GALILEU · e-ISSN 2184-1845 · Volume XXIII · Issue Fascículo 1-2 · 1st January Janeiro – 31st December Dezembro 2022 · pp. 63-79

ABSTRACT The scope of the research, related to the Brazilian pre-trial investigation, aims to verify whether obtaining of metadata and content data directly from a private storage establishment is in line with the Budapest Convention, European Union Law and the U.S. Cloud Act. This is relevant because, in most cases, it is only possible to determine who committed a crime and obtain evidence that can be used in Court, when electronic evidence, invariably stored abroad, are quickly collected. On the other hand, traditional mechanisms for mutual cooperation are considered obsolete to solve the problem.
KEYWORDS criminal investigation; digital evidence; non-essential MLA; obtaining directly from the private entity; Brazil and comparative law.

1. Introdução

O fenómeno da globalização, compreendido como "o facto de vivermos cada vez mais num único mundo, na medida em que os indivíduos, os grupos e as nações estão a tornar-se cada vez mais interdependentes" (GIDDENS, 2013, p. 131), produz impacto nos mais diversos campos da vida em sociedade, num processo de retroalimentação que é impulsionado pelo desenvolvimento tecnológico, especialmente pelo advento da *internet*, computadores, *smartphones* e seu amplo espectro, permitindo o fluxo de dados, voz e imagem, ao arrepio de quaisquer limitações territoriais existentes entre os países.

A par disso, a multiplicidade de empresas transnacionais, a economia eletrônica e a velocidade nos deslocamentos para superar grandes distâncias, influenciam nesse processo de *compressão do tempo/espaço*[3].

Inegavelmente, os avanços da computação e da tecnologia da informação transformaram e continuam transformando com rapidez exponencial todos os aspectos da vida moderna, constituindo-se em elementos essenciais para a economia e a sociedade. A utilização da *internet* e, especialmente das mídias sociais, *webmails* e aplicativos para uma gama infindável de situações tornou-se corriqueira em quase todo o planeta[4].

No entanto, concomitantemente aos benefícios econômicos, sociais, culturais e de lazer, essas tecnologias passaram a ser utilizadas também de maneira desvirtuada, como supedâneo para a criação de novos crimes, próprios deste ambiente[5] ou como ferramentas para transmudar a natureza, escala e alcance de crimes já conhecidos. Quando isso acon-

3 Expressão cunhada por David Harvey, *apud* Bauman (1999, p. 63).

4 Segundo a *International Telecommunication Union* (agência especializada das Nações Unidas), aproximadamente 4,9 bilhões de pessoas (63% da população mundial) estão usando a *internet*. Disponível em: *https://bit.ly/3QeKr4H (Consult. em 14 de agosto de 2022).*

5 Os designados cibercrimes. *v.g. denial of service* (DoS) e *distributed denial of service* (DDoS); *ransomwares*; propagação de vírus, etc.

GALILEU · e-ISSN 2184-1845 · Volume XXIII · Issue Fascículo 1-2 · 1st January Janeiro – 31st December Dezembro 2022 · pp. 63-79

tece, o ambiente virtual costuma ser o único lugar onde podem ser encontrados elementos para determinar quem cometeu um crime.

Especificamente, os serviços em rede podem ser fornecidos de qualquer espaço, dispensando infraestrutura física, pessoal ou instalações no país dos usuários. Eles também não carecem de local específico para o armazenamento de dados, que é eleito segundo as conveniências do provedor de serviços, majoritariamente no intento de reduzir custos, otimizar lucros, proteger dados e oferecer melhor acesso e desempenho.

Na consecução dessas estratégias empresariais, os fornecedores privados, percebendo a fragilidade da regulação estatal no ambiente virtual, comumente adotam dois caminhos: (a) prestam serviços em determinado país sem a presença de estabelecimento físico ou; (b) criam subsidiárias para funcionar no local, apenas com a função de vender serviços, mantendo o armazenamento sob o encargo de outro ente do grupo econômico, em país com a legislação que mais lhe beneficie. O intento é claro, maximizar as oportunidades, afastando qualquer empecilho em sentido contrário.

Por conseguinte, as provas aptas a elucidar delitos cometidos em determinado país, estão ordinariamente armazenados em território estrangeiro[6], sem conexão entre o caso sob investigação no Estado em questão e o Estado do local de armazenamento ou da sede principal do prestador de serviços, originando o que se tem chamado de *globalização das evidências criminais*.

De outro lado, os investigadores estão limitados aos seus territórios[7] e as formas tradicionais de obter provas em jurisdições alienígenas não são eficazes. Isso gera extrema dificuldade na promoção da justiça, ante a incapacidade estatal de proteger a vítima e os bens jurídicos agredidos.

Nesse diapasão, o Brasil tem buscado soluções jurídicas para enfrentar o problema. A questão que se coloca é aquilatar a adequação da postura brasileira frente aos instrumentos jurídicos previstos na Convenção de Budapeste, nos Estados Unidos da América (EUA) e na União Europeia (UE).

Em linha com o objeto da pesquisa, será realizada sucinta exposição jurídica do tema no Brasil, nas disposições da Convenção de Budapeste, no *Cloud Act* dos EUA e na legisla-

6 Ante a computação em nuvem, as maiores empresas globais mantêm *data centers* em múltiplos países, com armazenamento fracionado de dados e trânsito automatizado quase constantemente entre eles, no intuito de aprimorar o desempenho ante a diminuição da latência, por exemplo.

7 Smuha (2018, p. 85, tradução nossa) é contundente a respeito: "Embora os criminosos muitas vezes deixem evidências úteis *online* e sejam capazes de mover dados de um servidor localizado de um país para outro com o *clique* de um *mouse*, as forças policiais devem interromper sua busca na fronteira virtual e buscar assistência de outro estado. Se o objetivo é obter justiça criminal rápida, essa situação parece ridícula na melhor das hipóteses e perigosa para a sociedade na pior."

GALILEU · e-ISSN 2184-1845 · Volume XXIII · Issue Fascículo 1-2 · 1st January Janeiro – 31st December Dezembro 2022 · pp. 63-79

ção corretada da UE, para então verificar a existência de elementos comuns, em prol do direito fundamental à segurança e a justiça[8], estabelecendo critérios a serem observados por todos os Estados.

2. Abordagem no Brasil

No trato da questão de obtenção de provas eletrônicas envolvendo prestadores de serviços estrangeiros em funcionamento no Brasil, a Corte Especial do Superior Tribunal de Justiça (STJ), harmonizando a legislação federal, tem entendimento consolidado no sentido de que o local de armazenamento não afasta a jurisdição do país para requisitar diretamente o fornecimento de metadados ou dados de conteúdo, imprescindíveis a descoberta de crime ocorrido em território nacional, envolvendo brasileiros.

O *leading case*[9] que levou ao entendimento acima, tratava de recusa do *Google Brasil* em fornecer, diretamente às autoridades brasileiras, o conteúdo de *e-mails* trocados entre brasileiros investigados pela prática de crimes graves (associação criminosa, corrupção, lavagem de dinheiro *etc*), sob a justificativa que os dados estavam armazenados em território americano, ao abrigo da controladora *Google Inc*. Nesse passo, a subsidiária argumentou que além de não ter acesso ao conteúdo, a legislação americana proibia sua divulgação, salvo por meio da assistência jurídica mútua (MLA, sigla para *mutual legal assistance*).

Posteriormente, a Lei 12.965/14, conhecida como Marco Civil da *Internet* (MCI) regulou o assunto no Art. 11, *caput*, §§1.º e 2.º:

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
>
> § 1.º O disposto no *caput* aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.

8 O trabalho adota a concepção de "[...] plurinormatividade da segurança: [que] atravessa todo o ordenamento jurídico – [...] nacional e supranacional – e assume-se nele como fundamental para a vida em comunidade; e absorve, como bem a preservar e essencial ao desenvolvimento harmonioso da comunidade, o domínio público e o domínio privado do Direito." (VALENTE, 2012, p. 79).

9 STJ/Inq/784/DF, Relatora Ministra Laurita Vaz, DJe 28/08/13.

GALILEU · e-ISSN 2184-1845 · Volume XXIII · Issue Fascículo 1-2 · 1st January Janeiro – 31st December Dezembro 2022 · pp. 63-79

> § 2.º O disposto no *caput* aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.[10]

Como se percebe, o MCI alarga os critérios da jurisprudência, sujeitando as pessoas jurídicas estrangeiras à lei brasileira, ainda quando não tenham sede no Brasil, desde que prestem serviço no país, sempre que qualquer operação de coleta, armazenamento, guarda, tratamento de metadados ou dados de conteúdo tenha ocorrido em território nacional.

3. Abordagem na Convenção sobre Cibercrime

A *Convenção sobre Cibercrime* (Convenção de Budapeste)[11] [12], de caráter universal, prevê que as partes estabeleçam poderes e procedimentos para obter provas eletrônicas[13] e prestar assistência jurídica mútua, não limitada a crimes cibernéticos. Ainda, no Art. 18.1, "b", cria injunção para que as Partes ordenem ao fornecedor, que preste serviços no seu território, com ou sem sede física, a entrega de *dados de assinante* na sua posse ou sob seu controle[14]. Além disso, a Convenção prevê, nos artigos 16 e 17, ordens de preservação quando houver motivos para acreditar que os dados de computador são particularmente vulneráveis a perda ou modificação.

Todavia, os avanços tecnológicos e o incremento da complexidade supra referidos, vem exigindo maior celeridade na obtenção de provas eletrônicas, especialmente porque atualmente elas são imprescindíveis na maioria das infrações penais comuns.

Segundo dados compilados pelo Conselho da UE[15], **mais da metade de todas as investigações criminais atuais incluem uma solicitação transfronteiriça para acessar evidências eletrônicas,** como dados de identificação, textos, mensagens, e-mails ou

10 Antes dela, o Art. 11, §1.º da Lei de Introdução às normas do Direito Brasileiro e o Art. 21, parágrafo único do Código de Processo Civil Brasileiro preveem que a pessoa jurídica estrangeira que tiver agência, filial ou sucursal no Brasil, fica sujeita à lei nacional.

11 Convenção de Budapeste (ETS n.º 185) de 23 de novembro de 2001.

12 O Brasil somente aprovou o texto da Convenção em 16 de dezembro de 2021, por meio do Decreto Legislativo n.º 7. Registre-se que ainda não foram concluídos os trâmites necessários para internalização.

13 Para uma visão ampla sobre provas eletrônicas em grande parte dos Estados-Membros da UE [definição, procedimento nacional e internacional tanto para obtenção quanto para guarda; autoridade competente para execução, etc] ver o sítio: *https://bit.ly/3Jnku16*. Acesso em: 19 de jul. de 2022.

14 Para interpretação deste dispositivo, consultar a Nota de Orientação n.º 10, intitulada *Production orders for subscriber information (Article 18 Budapest Convention)*, emanada pelo *Cybercrime Convention Committee* (T-CY).

15 *Vide: E-evidence – cross-border access to electronic evidence: improving cross-border access to electronic evidence.*

GALILEU · e-ISSN 2184-1845 · Volume XXIII · Issue Fascículo 1-2 · 1st January Janeiro – 31st December Dezembro 2022 · pp. 63-79

aplicativos. E, as provas eletrônicas **são relevantes para aproximadamente 85% das investigações criminais**[16].

Ilustrativamente, os relatórios de transparência do *Facebook* (*Meta*) e do *Google*, concernentes a evolução do número de solicitações recebidas para fornecimento de provas eletrônicas por autoridades do Brasil e globalmente, são capazes de dimensionar o fenômeno:

***Facebook*/Brasil**

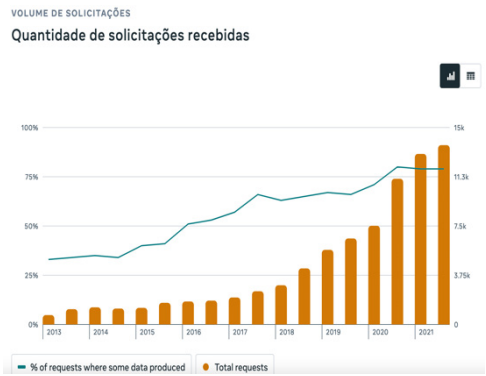

Figura 1. *Facebook. Transparency Center*. **Brazil**

***Google*/Brasil**

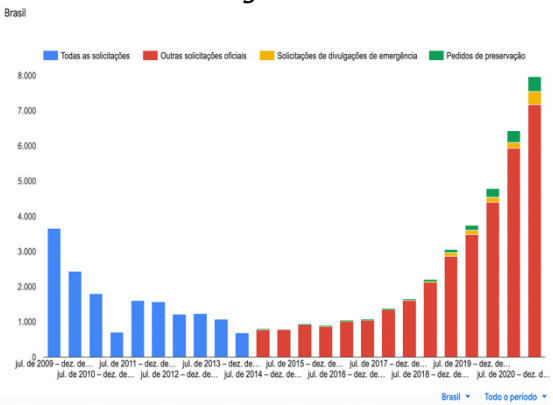

Figura 2. ***Google. Relatório de Transparência*. Brasil**

16 *Vide: Commission Staff Working Document Impact Assessment.*

GALILEU · e-ISSN 2184-1845 · Volume XXIII · Issue Fascículo 1-2 · 1st January Janeiro – 31st December Dezembro 2022 · pp. 63-79

Facebook/Global

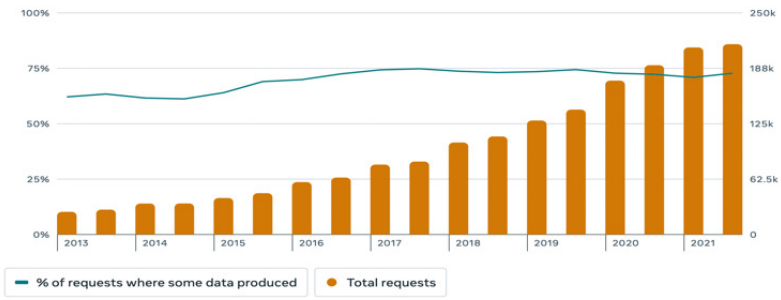

Figura 3. *Facebook*. Transparency Center. Global

Google/Global

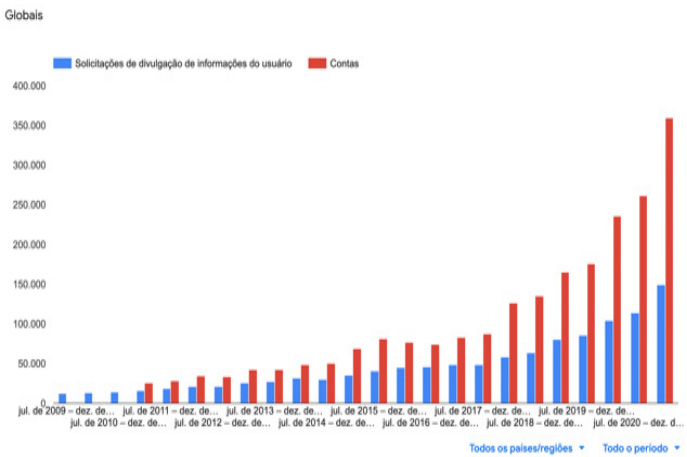

Figura 4. *Relatório de Transparência*. Solicitações globais.

GALILEU · e-ISSN 2184-1845 · Volume XXIII · Issue Fascículo 1-2 · 1st January Janeiro – 31st December Dezembro 2022 · pp. 63-79

Atenta a essa realidade, a Comissão da União Europeia propôs o segundo protocolo adicional à Convenção sobre Cibercrime [CETS n.º 224][17], firmado, até 10 de julho de 2022, por 24 (vinte e quatro) países[18] [19].

Em síntese, o segundo protocolo aborda a divulgação de informações de registro de nomes de domínio, medidas de cooperação direta com provedores de serviços para obtenção de informações de usuários, meios eficazes para obtenção de informações de usuários e dados de tráfego, cooperação imediata em emergências, ferramentas de assistência mútua, bem como salvaguardas para a preservação dos direitos humanos no ambiente digital (SANTOS, 2022, p.11).

4. Abordagem nos Estados Unidos da América

O *Cloud Act*[20], aprovado em março de 2018, pelos EUA, altera o *Stored Communications Act*, de 1986 (18 U.S. *Code Chapter* 121)[21], permitindo que as autoridades americanas obtenham prova eletrônica para fins criminais, independentemente do local onde o prestador do ser-

17 O *Preâmbulo* do mencionado protocolo corrobora o que vem se afirmando: "Reconhecendo a utilização crescente das tecnologias da informação e da comunicação, designadamente os serviços de internet, e o aumento da cibercriminalidade, que constitui uma ameaça para a democracia e o Estado de direito e que muitos Estados também consideram uma ameaça para os direitos humanos; Reconhecendo igualmente o número crescente de vítimas da cibercriminalidade e a importância de obter justiça para essas vítimas; Recordando que os governos têm a responsabilidade de proteger a sociedade e as pessoas contra a criminalidade não só fora de linha (*offline*), mas também em linha (*online*), nomeadamente através de investigações e ações penais eficazes; Cientes de que os elementos de prova de qualquer infração penal são cada vez mais armazenados em formato eletrónico em sistemas informáticos situados em jurisdições estrangeiras, múltiplas ou desconhecidas, e convencidos de que são necessárias medidas adicionais para obter licitamente esses elementos de prova, a fim de permitir uma resposta eficaz da justiça penal e defender o Estado de direito; Reconhecendo a necessidade de uma cooperação reforçada e mais eficaz entre os Estados e o setor privado, e que, neste contexto, é necessária maior clareza ou segurança jurídica para os prestadores de serviços e outras entidades no que diz respeito às circunstâncias em que podem responder a pedidos diretos das autoridades de justiça penal de outras Partes para a comunicação de dados eletrônicos; [...]."

18 Dentre eles, Portugal e, como não integrantes da UE: EUA, Chile, Colômbia, Japão e Marrocos, consoante o *Chart of signatures and ratifications of Treaty 224*.

19 O protocolo entrará em vigor no primeiro dia do mês seguinte ao termo de um período de três meses a contar da data em que 5 (cinco) Estados-Partes tenham manifestado seu consentimento em ficarem vinculadas ao mesmo (Art. 16.3 do segundo protocolo adicional a Convenção de Budapeste).

20 *U.S. Clarifying Lawful Overseas Use of Data Act*, H.R. 4943, 2018.

21 O *Stored Communications Act* (*SCA*), dispõe sobre o tratamento legal aplicável a comunicações armazenadas, vedando a divulgação de dados de conteúdo, exceto nas 8 (oito) exceções especificadas no §2702(b) do 18 *USC*, das quais, destacam-se: as situações de emergência envolvendo perigo de morte ou lesão grave de pessoa e; a exploração sexual e outros abusos de crianças e adolescentes, reportadas, no último caso, ao *National Center for Missing and Exploited Children* (*NCMEC*) (18 *USC* 2258A). Nessas situações, os dados de conteúdo são transmitidos diretamente as autoridades estrangeiras responsáveis pela persecução penal.

GALILEU · e-ISSN 2184-1845 · Volume XXIII · Issue Fascículo 1-2 · 1st January Janeiro – 31st December Dezembro 2022 · pp. 63-79

viço, sob sua jurisdição,[22] a mantenha armazenada (18 USC §2713)[23]. Ainda, prevê a possibilidade de países estrangeiros firmarem *acordos executivos* com os EUA [acordos bilaterais], permitindo que o *conteúdo* de comunicações de cidadãos não americanos e não residentes seja obtida diretamente junto aos prestadores de serviços com sede principal nos EUA[24].

Por outro lado, quanto aos metadados, subdivididos pela UE, em dado de *assinante,* de *acesso* e *transacional*, não há impedimento legal para que sejam fornecidos voluntariamente pelos provedores americanos diretamente as autoridades criminais do país onde prestam serviços.

Desse modo, a cooperação voluntária para fornecimento de dados que não sejam de conteúdo é recorrente com prestadores de serviços americanos. Mas sendo discricionária, despida de mecanismos legislativos cogentes para cumprimento e entrega tempestiva, o Estado requerente fica inteiramente a mercê do prestador de serviços[25] [26].

O *Cloud Act* não alterou esse panorama. Os acordos executivos firmados sob sua égide servem tão somente para eliminar os conflitos legais existentes entre as legislações dos países a que o prestador de serviço está submetido. Não são criadas obrigações ao provedor ou conferidos poderes coercitivos ao Estado requerente[27].

5. Abordagem na União Europeia[28]

Cuidando do tema proposto, traz-se à baila, a Diretiva 2000/31/CE do Parlamento Europeu e do Conselho, de 8 de junho de 2000, *relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio eletrônico, no mercado interno*, a qual, imperiosamente, deve ser analisada levando em conta as modificações a serem promovidas, brevemente, pelo *Digital Services Act* (*DAS*)[29], aplicável a qualquer plataforma digital que preste serviços

22 O que não se confunde com os prestadores sediados em seu território ou constituídos por americanos.

23 O *Cloud Act* vem na esteira do caso *Microsoft v. United States*, no qual a Suprema Corte foi provocada a decidir se o *SCA* obrigava a *Big Tech*, sob jurisdição estadunidense, a entregar dados armazenados no exterior, relativos a crime de tráfico de drogas cometido em solo americano. Com a superveniência do *Cloud Act*, o caso foi encerrado sem apreciação do mérito. Para aprofundamento acerca do litígio ver: DASKAL (2018).

24 As condições e procedimentos necessários para firmar o acordo podem ser consultados no ato, antes referido, que institui o *Cloud Act*.

25 Nas palavras de Palmieri (2021, tradução nossa): "Os provedores acabam se tornando os verdadeiros guardiões do poder de implementação do horizonte investigativo."

26 Segundo relatórios atuais de transparência do *Facebook* (*Meta*) e do *Google* o percentual de atendimento dos pedidos de autoridades brasileiras e globalmente, não atinge 70% e 80%, respectivamente.

27 Conforme consta no *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act* do Departamento de Justiça dos EUA.

28 Para uma análise abrangente da legislação relativa a proteção dos dados pessoais na UE, acompanhada de farta jurisprudência, consultar ficha temática do Tribunal de Justiça da UE (2021).

29 Proposta de Regulamento do Parlamento Europeu e do Conselho relativo a um mercado único de serviços digitais – COM(2020) 825 final – 2020/0361 (COD) já aprovado em primeira leitura pelo Parlamento e com expecta-

intermediários[30] a usuários residentes na UE, ainda que não tenha estabelecimento nos Estados-Integrantes.

O *DAS* reforça a obrigatoriedade do prestador de serviço, sem sede na UE, designar um representante legal [pessoa singular ou coletiva], para se fazer fisicamente presente num dos Estados-Membros [Art. 11], dotando-o de poderes para cumprir as ordens emanadas ao abrigo do regulamento.

Em consonância, o Regulamento Geral sobre a Proteção de Dados (RGPD)[31], no seu Art. 27 c/c Art. 3.2, também elenca o dever dos responsáveis pelo tratamento[32] [ou subcontratante] de dados de titulares [pessoas físicas] residentes no território da União, a designarem um representante num dos Estados-Membros, quando ali não estiverem sediados[33], independentemente do local onde os dados são tratados[34].

Com idêntica previsão da obrigatoriedade de designação de representante legal, segue a *proposta de diretiva do Parlamento Europeu e do Conselho que estabelece normas harmonizadas aplicáveis à designação de representantes legais para efeitos de recolha de provas em processo penal*[35], conforme previsão contida no Art. 3.2[36].

Assim, enquanto o *DAS* não entra em vigor e a *proposta de diretiva* supra não é aprovada, alguns Estados-Membros, com fundamento no Art. 3.4. da Diretiva 2000/31/CE, tem esta-

tiva de entrar em vigor no ano de 2024.

30 No Art. 2.º, "f", do aludido diploma legal, define-se *serviço intermediário* como: "um serviço de 'simples transporte' que consista na transmissão, através de uma rede de comunicações, de informações prestadas por um destinatário do serviço ou na concessão de acesso a uma rede de comunicações, – um serviço de 'armazenagem temporária' que consista na transmissão, através de uma rede de comunicações, de informações prestadas por um destinatário do serviço, que envolva a armazenagem automática, intermédia e temporária dessas informações, apenas com o objetivo de tornar mais eficaz a transmissão posterior das informações a outros destinatários, a pedido destes, – um serviço de 'armazenagem em servidor' que consista na armazenagem de informações prestadas por um destinatário do serviço a pedido do mesmo;".

31 Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, *relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*.

32 O Art. 4.2 do RGPD define *tratamento* como: "[...] uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição;".

33 Nos termos do Art. 3.2 do RGPD, a obrigação de designar representante, somente ocorre quando a atividade de tratamento tenha relação com: "a) A oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento; b) O controlo do seu comportamento, desde que esse comportamento tenha lugar na União." Estão excluídas da obrigação as situações constantes nos itens "a" a "d" do Art. 2.2 do RGPD.

34 Art. 3.1. do RGPD.

35 COM(2018) 226 final – 2018/0107 (COD).

36 Art. 3.2 do RGPD: "No caso dos prestadores de serviços que não se encontram estabelecidos na União, os Estados-Membros devem garantir que aqueles que operarem nos respetivos territórios designam, pelo menos, um representante legal na União, para receber e dar cumprimento a decisões e ordens emitidas por autoridades competentes dos Estados-Membros, para efeitos de recolha de provas em processo penal. O representante legal deve residir ou estar estabelecido num dos Estados-Membros em que o prestador de serviços opera."

GALILEU · e-ISSN 2184-1845 · Volume XXIII · Issue Fascículo 1-2 · 1st January Janeiro – 31st December Dezembro 2022 · pp. 63-79

belecido a obrigação das plataformas designarem representante legal em seu território, bem como outras medidas coercitivas[37].

Imperioso mencionar, por fim, a *proposta de regulamento do Parlamento Europeu e do Conselho relativo às ordens europeias de entrega e conservação de provas eletrônicas em matéria penal*[38] (*eEvidence*), a qual, na esteira da *Cloud Act* americana, oferece aos Estados-Membros da UE, uma alternativa diversa do MLA.

Na realidade, essa proposta, juntamente com a proposta de diretiva que obriga a *designação de representantes legais para efeitos de recolha de provas em processo penal* acima comentada, faz parte de um pacote legislativo que implementa dois instrumentos expeditos e simplificados para a colheita direta de provas eletrônicas pelas autoridades encarregadas da persecução penal: *a Ordem Europeia de Entrega de Provas* (OEEP) e a *Ordem Europeia de Conservação de Provas* (OECP)[39].

A OEEP abarca os dados de *assinante*, de *acesso*, *transacional* e de *conteúdo*[40], sendo que os últimos dois dispõem de condições e garantias acentuadas, uma vez que o Parlamento Europeu escalona o grau de afetação dos direitos fundamentais frente a cada uma das espécies[41].

6. Parâmetros comuns

A obtenção de provas eletrônicas para fins de investigação criminal é preocupação presente há várias décadas na comunidade internacional. Mas a demanda crescente, fluidez e imprescindibilidade de acesso em tempo útil[42], tem exercido forte pressão nos sistemas

37 Caso da Alemanha, que no §5.º n.º 2 da *Netzwerkdurchsetzungsgesetz* [*NetzDG*] prevê que os provedores de redes sociais devem nomear um destinatário autorizado a receber e responder pedidos de informações emitidos pelas autoridades criminais nacionais.

38 COM(2018) 225 final – 2018/0108 (COD).

39 *Vide*: *E-evidence – cross-border access to electronic evidence: improving cross-border access to electronic evidence*.

40 A definição de cada espécie de dados está prevista no Art. 2.º, itens "7" a "10".

41 Conforme explicita o "Considerando 23" da Proposta de Regulamento referida. Por exemplo, as ordens para produzir dados de assinantes e dados de acesso podem ser emitidas para qualquer infração penal, enquanto os dados transacionais e de conteúdo exigem que o crime tenha pena máxima igual ou superior a 3 (três) anos ou digam respeito aos seguintes crimes graves: (a) terrorismo (Diretiva 2017/541/UE); (b) fraude e a falsificação de meios de pagamento que não em numerário (Diretiva 2019/713/UE); (c) combate ao abuso e à exploração sexual de crianças e à pornografia infantil (Diretiva 2011/93/UE) e; (d) ataques contra os sistemas de informação (Diretiva 2013/40/UE).

42 As provas eletrônicas, como é sabido, são voláteis e podem facilmente ser alteradas e eliminadas. O cenário se agravou após o julgamento do caso *Digital Rights Ireland* (Acórdão de 8 de abril de 2014, proc. C-293/12 e C-594/12), ocasião que o TJUE invalidou a Diretiva n.º 2006/24/CE, do Parlamento Europeu e do Conselho, de 15 de março de 2006, afastando a obrigação dos prestadores de serviço armazenarem os dados eletrônicos por um período mínimo.

de justiça criminal domésticos, especialmente porque o caminho da cooperação jurídica mútua tem se mostrado anacrônico.

A necessidade premente, obstaculizada pelo armazenamento de dados em nuvem, com *data centers* situados em território estrangeiro e estratagemas societários que cindem as funções de uma pessoa jurídica prestadora de serviços, por meio de subsidiárias, tem levado a uma reação dos Estados quanto a artificial maneira de definir o território competente, em evidente prejuízo a soberania e a jurisdição[43].

A coletânea de instrumentos jurídicos trazidos à lume, é exemplo disso. A Convenção de Budapeste e os EUA, por meio do *Cloud Act*, assentam que a jurisdição das partes e a americana, respectivamente, não são afetadas pelo local de armazenamento de dados eletrônicos. Na mesma toada, a Diretiva 2000/31/CE, no seu Art. 3.4, já permitia que os Estados-Membros obtivessem provas eletrônicas independentemente do local onde estão armazenadas, culminando, recentemente, com a expressa previsão do *eEvidence*[44].

Outra solução engendrada na UE, conforme relatado, tem a ver com a obrigatoriedade dos prestadores de serviço, que atuam no território dos seus integrantes,[45] designar um representante legal num dos Estados-Membros[46]. É assim no *RGPD*, no *DAS* e na *proposta de diretiva do Parlamento Europeu e do Conselho que estabelece normas harmonizadas aplicáveis à designação de representantes legais para efeitos de recolha de provas em processo penal*.

Em comum, os Estados-Membros da UE e os EUA, para não verem sacrificado o direito fundamental à segurança[47], enveredaram por buscar diretamente, junto aos prestadores de serviço, as provas digitais relativas aos crimes que são competentes para investigar[48].

43 Ramos (2016) chama de *Direito Transnacional anárquico* a estimulação mecânica e falsamente neutra promovida pelos agentes econômicos privados, visando manipular os elementos de *conexão* ou de fixação da jurisdição tradicionais do Direito Internacional Privado a fim de proteger seus interesses. Como exemplo, cita o armazenamento de dados em território da preferência da empresa (*forum shopping*) e a criação de subsidiárias nos países onde presta serviço.

44 "[...] a aplicação do presente regulamento não deverá depender da localização efetiva do estabelecimento do prestador ou da instalação de tratamento ou armazenamento dos dados em causa." (Considerando 17).

45 Para caracterizar a prestação de serviço no Estado-Membro, exige-se uma *ligação substancial* que, além da possibilidade de as pessoas utilizarem o serviço, envolve a *orientação das atividades* a um dos membros da UE, tais como: utilização do idioma, moeda; publicidade local ou na língua do local; uso de extensão de um dos Estados-Membros (ccTLD).

46 A presença de um representante legal na UE resolve os problemas relacionados à execução, vez que eles ficam vinculados à sua legislação e, na hipótese de descumprimento, podem ser penalizados.

47 Acerca da importância deste direito fundamental, Valente (2012, p. 80) ensina: "A extensibilidade conceptual da topologia segurança significa a subordinação a uma topologia valorativa real de construção cognitiva epistemológica e axiológica como bem vital (mas não absoluto) de toda a comunidade (nacional e supranacional). Uma comunidade desprovida de segurança é uma comunidade desguarnecida de desenvolvimento e de crescimento do ser humano."

48 *A fortiori* porque podem ser acessados de qualquer lugar, o que leva Daskal (2015) a apontar que os dados armazenados nas nuvens são tratados como *a-territoriais*.

GALILEU · e-ISSN 2184-1845 · Volume XXIII · Issue Fascículo 1-2 · 1st January Janeiro – 31st December Dezembro 2022 · pp. 63-79

Destarte, nas situações em que os dados eletrônicos circunscritos a nacionais [membros no caso da UE] e residentes suspeitos da prática de crime em determinado país, o fato de as provas estarem armazenadas em outro território não tem o condão de impedir sua obtenção direta pelas autoridades competentes.

Paradoxalmente, a UE e os EUA refutam a aplicação de idêntico raciocínio para países terceiros. No caso dos EUA, caso outro Estado queira acessar *dados de conteúdo* armazenado em seu território ou de prestadores sujeitos a sua jurisdição, o caminho apontado é firmar um *acordo executivo*. A UE, por sua vez, indica o *MLA* para a obtenção de qualquer espécie de dado[49]. Não importa sequer que se trate de *caso exclusivamente doméstico*, no qual o prestador de serviço atua no Estado requerente e os dados tenham sido ali coletados, tratados ou recebidos.

O abuso de direito da UE e dos EUA neste ponto é manifesto, ainda que com maior ênfase para a primeira[50]. Embora assentem possuírem jurisdição para requisitar diretamente provas eletrônicas nas situações supra, constrangem os prestadores de serviço a não aceitarem requisições idênticas de países terceiros. Quer dizer, sem qualquer vínculo com o dado [salvo o armazenamento em seu território] ou com o crime investigado, aniquilam o direito fundamental à segurança[51] e a soberania territorial de outros países na aplicação das regras penais[52], caracterizando o que se convencionou chamar de ***guarda-chuva sueco***[53]**,** em alusão a um foro exorbitante que se afasta da ideia de acesso à Justiça.

49 Notadamente após a decisão do *Caso Schrems II* (*Privacy Shield*) (Processo n.º C-311/18 do TJUE), a doutrina tem afirmado que a UE vem se aproximando dos modelos autoritários da Rússia e China, assumindo, disfarçadamente, uma política de *localização de dados* ao bradar que os dados europeus devem permanecer na Europa. Concretamente, depois do julgamento do *Caso Schrems II*, a Autoridade de Proteção de Dados de Berlim emitiu uma declaração solicitando aos provedores de serviços sediados em Berlim, que armazenam dados pessoais nos EUA, para transferir os mesmos para a Europa e parar de transferir dados para os EUA até que o quadro jurídico seja reformado (ABRAHA, 2021).

50 No caso dos EUA a limitação diz respeito apenas a *dados de conteúdo* que podem ser obtidos, sem a necessidade de MLA caso seja firmado um acordo executivo. Contudo, dados de nacionais e residentes americanos não podem ser obtidos diretamente em nenhuma hipótese. A recíproca não é verdadeira.

51 A UE, no *Considerando 8* da *eEvidence*, manifesta plena consciência disso: "[...] a obtenção de provas eletrônicas através dos canais de cooperação judiciária é muitas vezes morosa, levando mais tempo do que aquele durante o qual os indícios poderão estar disponíveis." (grifo nosso)

52 A UE igualmente tem consciência da *obrigação positiva* de implementar investigações criminais eficazes, sob pena de violar o Art. 8.º da Convenção Europeia dos Direitos dos Homens/CEDH. Nesse sentido, consultar o *Guide on Article 8 of the European Convention on Human Rights*. O Tribunal Europeu de Direitos do Homem (TEDH), no caso KU *v*. Finlândia, reputou violado o Art. 8.º do CEDH, devido à falta de um quadro legislativo adequado apto a proteger a vítima e fornecer uma resposta efetiva da justiça criminal, uma vez que ao atribuir primazia absoluta a privacidade e a proteção de dados, ressentiu-se de meios aptos a descoberta da autoria delitiva.

53 Em alusão ao Capítulo 10, Seção 3, do Código de Processo Judicial da Suécia que prevê que uma pessoa poderá ser demandada no país se possuir qualquer bem móvel ou imóvel lá situado. A partir daí, é jocosamente dito que se um estrangeiro esquecer um guarda-chuva no aeroporto de Estocolmo, poderá ser julgado pelas Cortes locais em demanda de cobrança, ainda que a obrigação e o credor não tenham qualquer vínculo com o país.

GALILEU · e-ISSN 2184-1845 · Volume XXIII · Issue Fascículo 1-2 · 1st January Janeiro – 31st December Dezembro 2022 · pp. 63-79

Portanto, as balizas que a UE e os EUA adotam para si nesta matéria, deve servir, sem distinções, para todos os demais países, inclusive o Brasil[54]. Isso se traduz em dar primazia ao *princípio da territorialidade objetiva*[55] na definição do território competente para requisição direta de provas digitais, salvaguardando a jurisdição e a soberania do país onde o prestador de serviços participa da economia local e dirige ativa e voluntariamente suas atividades econômicas para os consumidores locais[56].

7. Conclusão

À luz dos desafios discutidos acima, compreende-se que as investigações criminais domésticas eficazes geralmente dependem de o país investigador ter autoridade sob a legislação interna para obter dados eletrônicos que os prestadores de serviços, sujeitos à sua jurisdição, possuem, inclusive fora de suas fronteiras, desde que relacionadas com seus nacionais e residentes.

Destarte, o aparente conflito de jurisdição na produção probatória é solucionado ao afastar o fictício vínculo criado com o país estrangeiro, decorrente de estratégia empresarial deturpadora dos instrumentos do Direito Internacional Privado.

Assim sendo, a realidade deve se sobrepor as manipulações, a fim de reconhecer os efetivos *elementos de conexão* e a *maior proximidade jurídica* incidentes no caso concreto. Do contrário, por via transversa, a fixação ou afastamento da soberania de um país estaria ao talante de entidade empresarial que esgarça os limites da autonomia da vontade, ofendendo a ordem jurídica interna, em detrimento insuportável do direito fundamental à segurança e a justiça.

A par disso, o critério de jurisdição alicerçado exclusivamente no local de armazenamento dos dados, consoante aludido, esbarra em questão de ordem operacional inerente a computação em nuvem, haja vista que, neste modelo, é praxe sejam os dados particionados em *data centers* localizados em países distintos e migrem constantemente entre eles. De mais, o dado eletrônico perseguido, regra geral, foi coletado ou recebido no Estado requente e dele pode ser acessado pelo prestador de serviço.

54 O Supremo Tribunal Federal irá julgar a Ação Declaratória de Constitucionalidade (ADC) n.º 51 onde, por via transversa, entidade que congrega empresas de tecnologia de informação, quer ver declarado o MLA como ferramenta necessária, nos casos de armazenamento extraterritorial, para obtenção de *dados de conteúdo*. Algo que, conforme verificado, segue na contramão das movimentações da UE e dos EUA.

55 *Vide* a respeito, acórdão da Suprema Corte da Bélgica (*Cour de Cassation*), de 1 de dezembro de 2015, que obrigou o *Yahoo!* a fornecer dados eletrônicos em investigação criminal, vez que presente o *princípio da territorialidade objetiva* ante a utilização de domínio "be", idioma local, *pop-up* com anúncios com base em geolocalização, serviço de atendimento ao cliente direcionado aos usuários belgas etc.

56 Ver nota 44.

GALILEU · e-ISSN 2184-1845 · Volume XXIII · Issue Fascículo 1-2 · 1st January Janeiro – 31st December Dezembro 2022 · pp. 63-79

Justamente pelo exposto, as providências da UE e dos EUA ligadas ao legítimo interesse de possuírem instrumentos que propiciem o acesso, em tempo hábil, às provas eletrônicas indispensáveis a uma investigação eficaz, garantindo o direito fundamental à segurança e a justiça numa sociedade democrática e, em última medida, o respeito aos Direitos do Homem – gravados na Declaração Universal dos Direitos Humanos (Art. 3.º); Convenção Europeia dos Direitos dos Homens (Art. 8.º) e na Convenção Americana sobre Direitos Humanos (Art. 7.º) – deve ser reconhecido aos demais Estados, sob pena de incorrerem em abuso de direito.

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*, v. 29, 2 ed. 2021, p. 118-153. Disponível em: https://bit.ly/3KJoObI. Acesso em: 15 de ago. 2022.

BAUMAN, Zygmunt. *Globalização: as consequências humanas*. Rio de Janeiro: Jorge Zahar Editor, 1999.

BRASIL. *Decreto Legislativo n.º 7, de 16 de dezembro de 2021*. Aprova o texto da Convenção sobre o Crime Cibernético, celebrada em Budapeste, em 23 de nov. de 2001. Disponível em: https://bit.ly/3uDtSav. Acesso em: 6 de jul. 2022.

BRASIL. *Decreto-Lei n.º 4.657, de 4 de setembro de 1942*. Lei de Introdução às normas do Direito Brasileiro. Disponível em: https://bit.ly/2Zr7a48. Acesso em 13 de ago. 2022.

BRASIL. *Lei 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: https://bit.ly/3R3IhpA. Acesso em: 13 de ago. 2022.

BRASIL. *Lei 13.105, de 16 de março de 2015*. Código de Processo Civil. Disponível em: https://bit.ly/3KDJYHU. Acesso em: 13 de ago. 2022.

BRASIL. Superior Tribunal de Justiça. *Inquérito n.º 784/DF*. Relatora Ministra Laurita Vaz. Disponível em: https://bit.ly/3RehtD6. Acesso em: 16 de ago. 2022.

BRASIL. Supremo Tribunal Federal. *Ação Declaratória de Constitucionalidade (ADC) n.º 51*. Relator Ministro Gilmar Mendes. Disponível em: https://bit.ly/3ADbG3e. Acesso em: 10 de ago. 2022.

BELGIQUE. Court de Cassation. *Arrest N.20151201-1 (P.13.2082.N)*, Raadsheer Erwin Francis, 1/12/2015. Disponível em: https://bit.ly/3RdLym2. Acesso em: 12 de ago. 2022.

CONSELHO DA UNIÃO EUROPEIA. *Segundo Protocolo Adicional à Convenção sobre o Cibercrime relativo ao reforço da cooperação e da comunicação de provas eletrônicas*. Disponível em: https://bit.ly/3PdtLKL. Acesso em: 5 de jul. 2022.

COUNCIL OF EUROPE. *Chart of signatures and ratifications of Treaty 224*. Disponível em: https://bit.ly/3c3crtr. Acesso em: 10 de jul. 2022.

COUNCIL OF EUROPE. *Convenção Europeia dos Direitos do Homem*. Disponível em: https://bit.ly/3RiwbJi. Acesso em: 23 de jul. 2022.

COUNCIL OF EUROPE. *Convention On Cybercrime*. Versão em português. Disponível em: https://bit.ly/3CxuuTM. Acesso em: 20 de jul. 2022.

COUNCIL OF EUROPE. *Cybercrime Convention Committee (T-CY)*. Production orders for subscriber information (Article 18 Budapest Convention). Disponível em: https://bit.ly/3Khfg7A. Acesso em: 28 de jul. 2022.

DASKAL, Jennifer C. The Un-Territoriality of Data. *The Yale Law Journal*, 326 (2015). Disponível em: https://bit.ly/3B1wXF1. Acesso em: 4 de ago. 2022.

DASKAL, Jennifer C. Microsoft Ireland, the CLOUD Act, and International Lawmaking 2.0. *The Stanford Law Review* (2018). Disponível em: https://stanford.io/3pPxzHt. Acesso em: 4 de ago. 2022.

DIRECTIVA 2000/31/CE DO PARLAMENTO EUROPEU E DO CONSELHO, de 8 de junho de 2000. *Directiva sobre comércio electrónico*. Disponível em: https://bit.ly/3vH8f9I. Acesso em: 23 de jul. 2022.

EUROPEAN COMMISSION. *E-evidence* – cross-border access to electronic evidence: improving cross-border access to electronic evidence. Disponível em: https://bit.ly/3c4Ys6V. Acesso em: 5 de ago. 2022.

EUROPEAN COMMISSION. *Commission Staff Working Document Impact Assessment* {SWD(2018) 118 final}, 17/4/2018: Accompanying the document {COM(2018) 225 final} – {COM(2018) 226 final}. Disponível em: https://bit.ly/3eioILJ. Acesso em: 14 de ago. 2022.

EUROPEAN COURT OF HUMAN RIGHTS. *Guide on Article 8 of the European Convention on Human Rights*. Disponível em: https://bit.ly/2GPofwr. Acesso em: 23 de jul. 2022.

EUROPEAN COURT OF HUMAN RIGHTS. *Case of KU v. Finland* (2872/02), 02/12/2018. Disponível em: https://bit.ly/3T7PwOQ. Acesso em: 23 de jul. 2022.

EUROPEAN JUDICIAL NETWORK. *EJN Fiches Belges on Electronic Evidence* – National Legal and practical information provided by the Contact Points. Disponível em: https://bit.ly/3Jnku16. Acesso em: 19 de jul. 2022.

FACEBOOK (META). *Transparency Center*. Brazil. Disponível em: https://bit.ly/3CoryZU. Acesso em: 14 de ago. 2022.

FACEBOOK (META). *Transparency Center*. Global overview. Disponível em: https://bit.ly/3QFm2GD. Acesso em: 14 de ago. 2022.

GIDDENS, Anthony. *Sociologia*. 9. ed. rev. e atual. Lisboa: Fundação Calouste Gulbenkian, 2013.

GOOGLE. *Relatório de Transparência*. Brasil. Disponível em: https://bit.ly/3QOvbwt. Acesso em: 14 de ago. 2022.

GOOGLE. *Relatório de Transparência*. Solicitações globais. Disponível em: https://bit.ly/3PT546o. Acesso em: 14 de ago. 2022.

GOVERNMENT OF SWEDEN. *The Swedish Code of Judicial Procedure*. Disponível em: https://bit.ly/3QeFSal. Acesso em: 15 de ago. 2022.

MITSILEGAS, Valsamis. The privatisation of mutual trust in Europe's area of criminal justice: The case of e-evidence. *In: Maastricht Journal of European and Comparative Law*, vol. 25 (3), 2018, p. 263-265. Disponível em: https://stanford.io/31z05By. Acesso em: 13 de ago. 2022.

NAÇÕES UNIDAS. Declaração Universal dos Direitos Humanos. 1948. Disponível em: https://bit.ly/3eMYlOW. Acesso em: 20 de ago. 2022.

PALMIERI, Paolo. *L'acquisizione delle prove elettroniche, la voluntary disclosure dei providers, e l'ordine europeo di produzione e conservazione dell'e-evidence in materia penale.* Disponível em: https://bit.ly/3AvUAE2. Acesso em: 16 de ago. 2022.

PARLAMENTO EUROPEU E DO CONSELHO. Proposta de Regulamento do Parlamento Europeu e do Conselho relativo a um mercado único de serviços digitais – *COM(2020) 825 final – 2020/0361 (COD).* Disponível em: https://bit.ly/30XOAyN. Acesso em: 25 de jul. 2022.

PARLAMENTO EUROPEU E DO CONSELHO. Proposta de regulamento do Parlamento Europeu e do Conselho relativo às ordens europeias de entrega e conservação de provas eletrônicas em matéria penal – *COM(2018) 225 final – 2018/0108* (COD). Disponível em: https://bit.ly/3vGI9nz. Acesso em: 26 de jul. 2002.

RAMOS, André de Carvalho. Direito internacional privado e o direito transnacional: entre a unificação e a anarquia. In: *Revista de Direito Internacional*, v. 13, n.º 2, 2016. Disponível em: https://bit.ly/3e4dXg6. Acesso: 10 de ago. 2022.

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, *relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*. Disponível em: https://bit.ly/2EfI4tr. Acesso em: 16 de jul. 2022.

REPÚBLICA FEDERAL DA ALEMANHA. *Netzwerkdurchsetzungsgesetz* [NetzDG]. Disponível em: https://bit.ly/3p0pcZ7. Acesso em: 2 ago. 2022.

SANTOS, Bruna Martins dos. Convenção de Budapeste sobre o cibercrime na América Latina: uma breve análise sobre adesão e implementação na Argentina, Brasil, Chile, Colômbia e México. Chile: *Derechos Digitales América Latina*, maio de 2022. Disponível em: https://bit.ly/3IqpocY. Acesso em: 10 de jul. 2022.

SMUHA, Nathalie A. Towards the EU Harmonization of Access to Cross-Border E-Evidence: Challenges for Fundamental Rights & Consistency. *European Criminal Law Review*, vol. 8(1), p. 83-115, 2018. Disponível em: https://bit.ly/3wAk7e6. Acesso em: 12 de ago. 2022.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPÉIA. Ficha temática: proteção dos dados pessoais. nov. 2021. Disponível em: https://bit.ly/3gr7f54. Acesso em: 18 de ago. 2022.

UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. *Digital Rights Ireland* (Processos C-293/12 e C-594/12), de 8 de abril de 2014. Disponível em: https://bit.ly/3elPWBv. Acesso em: 28 de jul. 2022.

UNITED NATIONS. International Telecommunication Union. *Measuring digital development*: Facts and figures 2021 Disponível em: https://bit.ly/3QeKr4H. Acesso em: 14 de ago. 2022.

U.S. DEPARTMENT OF JUSTICE. *Promoting Public Safety, Privacy, and the Rule of Law Around the World*: The Purpose and Impact of the CLOUD Act. Disponível em: https://bit.ly/3KCTkDO. Acesso em: 8 de ago. 2022.

U.S. GOVERNMENT. *Clarifying Lawful Overseas Use of Data Act*, H.R. 4943, 2018. Disponível em: https://bit.ly/2CLCOwO. Acesso em: 1 de ago. 2022.

U.S. GOVERNMENT. *18 U.S.C. 121* – Stored Wire and Electronic Communications and Transactional Records Access. Disponível em: https://bit.ly/3A5FHIt. Acesso em: 2 de ago. 2022.

U.S. Supreme Court of the United States. *84 U. S. (2018)*. Disponível em: https://bit.ly/2HEJBMR. Acesso em: 8 de ago. 2022.

VALENTE. Manuel Monteiro Guedes. Cooperação Judiciária em Matéria Penal no Âmbito do Terrorismo. in BRANDÃO, Ana Paula (Coord.). *A União Europeia e o Terrorismo Transnacional*. Coimbra: Almedina, 2010.

VALENTE. Segurança: bem jurídico supranacional. *JANUS.NET, e-journal of International Relations*. vol. 3, n.º 2, 2012. Disponível em: https://bit.ly/3B7AdPd (Consult. em 23 de julho de 2022).