Centro Universitário de Brasília - UniCEUB
Faculdade de Ciências Jurídicas e Sociais - FAJS
Curso de Bacharelado em Direito

MARIA FERNANDA DE SOUZA GOMES

A INVESTIGAÇÃO DE CIBERCRIMES E A COOPERAÇÃO INTERNACIONAL: O TRÂNSITO DE DADOS E O ADVENTO DO *CLOUD ACT*.

BRASÍLIA
2021

MARIA FERNANDA DE SOUZA GOMES

A INVESTIGAÇÃO DE CIBERCRIMES E A COOPERAÇÃO INTERNACIONAL: o trânsito de dados e o advento do *Cloud Act.*

Monografia apresentada como requisito parcial para obtenção do título de Bacharel em Direito pela Faculdade de Ciências Jurídicas e Sociais - FAJS do Centro Universitário de Brasília (UniCEUB).

Orientador(a): Prof. Me. José Carlos Veloso Filho

BRASÍLIA
2021

MARIA FERNANDA DE SOUZA GOMES

A INVESTIGAÇÃO DE CIBERCRIMES E A COOPERAÇÃO INTERNACIONAL: o trânsito de dados e o advento do *Cloud Act.*

Monografia apresentada como requisito parcial para obtenção do título de Bacharel em Direito pela Faculdade de Ciências Jurídicas e Sociais - FAJS do Centro Universitário de Brasília (UniCEUB).

Orientador(a): Prof. Me. José Carlos Veloso Filho

BRASÍLIA, ___ de _____ de 2021

BANCA AVALIADORA

_____

Professor(a) Orientador(a)
Prof. Me. José Carlos Veloso Filho

_____

Professor(a) Avaliador(a)

Dedico e agradeço à Deus. Agradeço também aos meus pais, meu eterno e mais bonito amor.

Por fim, agradeço ao meu orientador, pela atenção e dedicação.

RESUMO

Autora: Maria Fernanda de Souza Gomes[1]

Resumo: A presente monografia pretende averiguar a investigação criminal dos cibercrimes, colocando em evidência a cooperação internacional para o trânsito de dados. Sabe-se que, no âmbito digital da *internet*, deve-se atentar à diversos dados eletrônicos para apuração dos crimes, sendo assim, caracteriza-se um dilema entre o uso de dados e a proteção de dados. Dessa forma, buscam-se formas de cooperação, de maneira que, não seja infringida a lei ao obter os dados para investigação criminal. Portanto, intenta-se, aqui, observar e conceituar as provas na investigação de cibercrimes. Busca-se, de igual maneira, averiguar a legislação brasileira sobre o tema proposto, para, por fim, analisar o trânsito de dados por meio da cooperação internacional para investigação de cibercrimes, explicitando o posicionamento do Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional na Ação Declaratória de Constitucionalidade n° 51 acerca do Acordo de Assistência Judiciária em Matéria Penal entre o Brasil e os Estados-Unidos, apresentando, posteriormente, as vantagens dos acordos executivos delimitados na lei norte-americana, *Cloud Act*. A pesquisa se trata de uma pesquisa documental e bibliográfica qualitativa, observando a doutrina jurídica, artigos científicos, legislação, entre outros meios bibliográficos para a análise adequada do tema proposto. Pretende-se, portanto, analisar, à luz dos aspectos materiais e processuais, a investigação criminal dos cibercrimes e a cooperação internacional para o trânsito de dados, que propiciou a criação de um mecanismo de acesso conjunto a informações eletrônicas, os acordos executivos por meio do *Cloud Act*.

Palavras-chave: Cibercrimes; Investigação Criminal Digital; Uso de dados; Trânsito de dados; Cooperação internacional

[1] Bacharelanda em Direito pela Faculdade de Ciências Jurídicas e Sociais do Centro Universitário de Brasília. E-mail: mfsg.98@gmail.com

SUMÁRIO

INTRODUÇÃO

O desenvolvimento da *internet* trouxe avanços consigo, tais como a descentralização, a distribuição de redes em diversos locais do mundo e a velocidade na troca de informações, relacionando-se intrinsecamente com a área do Direito, visto que, pelas vantagens trazidas pelo anonimato e pela conexão em rede de alta velocidade, os crimes virtuais crescem e as fronteiras de jurisdição se esbarram, impondo um novo desafio à investigação penal.

A investigação dos cibercrimes e a busca por provas são áreas afetadas pelo avanço tecnológico na medida em que a dificuldade e a diversidade de dados necessários para apuração dos criminosos virtuais necessitam de uma colaboração internacional, por meio de mecanismos que busquem identificar os diversos infratores. Contudo, sabe-se que, para a investigação no âmbito digital, é necessário examinar um grande volume de dados eletrônicos, ressaltando o dilema entre o uso de dados e a proteção destes. Dessa forma, fica evidente a necessidade da utilização de diversas formas de cooperação internacional, buscando, entretanto, que não seja infringida a lei doméstica ao obter os dados para investigação criminal.

Nesse contexto, no Brasil, o tema vem sendo tratado desde 2012, quando se observou a primeira lei brasileira que tratou do crime cibernético, a Lei 12.737 de 30 de novembro de 2012, apelidada Lei Carolina Dieckman, que dispôs sobre crimes de invasão de dispositivo informático, além de modificar outros dispositivos do Código Penal, evidenciando o direito à privacidade e intimidade do indivíduo. Necessita-se ressaltar, de igual forma, que o âmbito do Direito Digital surgiu com o Marco Civil da Internet, Lei 12.965 de 23 de abril de 2014, que trata das relações, garantias, deveres e direitos dos indivíduos no que tange ao uso da *internet* no Brasil. Posteriormente, foi elaborada, ainda, a Lei Geral de Proteção de Dados Brasileira, Lei 13.709 de 14 de agosto de 2018, que dispôs sobre outra área do Direito Digital, a proteção de dados pessoais, visando fortalecer os direitos de liberdade e privacidade.

Constata-se que a tentativa de disciplinar o âmbito digital é recente, caracterizando um tema importante, tendo em vista que o debate acerca do uso de dados pessoais tem se difundido amplamente perante o ordenamento jurídico. Com a multiplicação dos cibercrimes e a velocidade de aparecimento e desaparecimento de informações de cunho pessoal na esfera virtual, os dados vêm sendo criados aos milhares por dia, tornando as investigações dos crimes virtuais complexas e exaustivas.

Assim, juntam-se dois aspectos que possuem grande relevância, a dificuldade da investigação digital dos cibercrimes e sua relação com o trânsito de dados, observando instrumentos de cooperação internacional e legislações de proteção de dados pessoais. Posto isso, indaga-se como problema de pesquisa: Quais aspectos, materiais e processuais, delimitam a cooperação internacional para a investigação de cibercrimes? Qual o posicionamento do Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional observado pela Ação Declaratória de Constitucionalidade n° 51 em relação ao Acordo de Assistência Judiciária em Matéria Penal entre o Brasil e os Estados Unidos?

Durante o desenvolvimento da pesquisa, seguem-se as observações e pontuações do Direito Processual Penal, relacionando à nova área do Direito Digital e Direito Internacional. Tem-se essa área como norte de pesquisa tendo em vista que o foco do trabalho trata da investigação de cibercrimes, sendo, portanto, uma área processual. Ainda, observa-se a relação da investigação cibernética com o trânsito de dados por cooperação, envolvendo o âmbito internacional, além da nova área do Direito Digital, tendo em vista que se pretende tratar acerca do uso e da proteção de dados.

De acordo com o Relatório de Cibercrimes de Janeiro-Junho de 2020, publicado pela LexisNexis Risk Solutions baseado nos ataques dos crimes virtuais globais, o Brasil se encontra em 3° lugar na lista de países que mais contribuem em volume para os ataques cibernéticos iniciados por humanos[2]. Ressalta-se, ainda, que a maioria dos órgãos federais e estaduais, no Brasil, se utilizam da *internet* para a execução de suas atividades. Nesse âmbito, ainda recentemente, no dia 3 de novembro de 2020, constatou-se um ataque *hacker* ao Superior Tribunal de Justiça, levando o órgão a reestabelecer totalmente sua rede tecnológica para solucionar o problema, o que acarretou prejuízos, ante a necessidade do cancelamento de sessões de julgamento, entre outras medidas[3].

Destaca-se o autor Cláudio Adriano Bomfati e Armando Kolbe como nortes teóricos para as considerações que aqui serão tecidas. De acordo com Bomfati e Kolbe, os crimes cibernéticos podem ser definidos como: “crime cibernéticos (ou crime informático, cibercrime, crime digital, e-crime) é uma modalidade de conduta, na qual ocorre a utilização de algum

[2] LEXISNEXIS RISK SOLUTIONS CYBERCRIME REPORT. **The changing face of cybercrime.** Digital Identity Network, Janeiro-Junho 2020. Relatório.

[3]Turmas remarcam sessões previstas para esta terça-feira (10), **Superior Tribunal de Justiça,** 09/11/2020. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/09112020-Turmas-remarcam-sessoes-previstas-para-esta-terca-feira--10-.aspx Acesso em: 25/11/2020

recurso da tecnologia da informação como meio de realizar a ilicitude”[4]. O autor, portanto, segue a definição proposta na Convenção Sobre o Cibercrime de Budapeste (2001) que definiu os cibercrimes como “actos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta desses sistemas, rede e dados”[5].

Além do norte teórico, faz-se necessário abordar outra autora que se debruça sobre o tema da investigação cibernética, qual seja, Dheneb Martins. A presente autora se utiliza das definições trazidas por Carla Rodrigues Araújo de Castro e Maria dela Luz Lima, convergindo para o seguinte conceito: “cibercrimes são todos aqueles crimes que envolvem os computadores (aqui, leia-se todo meio tecnológico no qual seja possível a utilização da *internet*) ou aqueles nos quais suas técnicas ou funções sejam utilizadas como fim, meio ou método”[6]. Dessa forma, observa-se que as conceituações dos crimes virtuais se demonstram homogêneas, tendendo à uma linha de pensamento formada.

Sobre crimes cibernéticos, pode-se abordar, semelhantemente, o autor Damásio E. Jesus que destaca que:

> Conceituamos crime informático como o fato típico e antijurídico cometido por meio da ou contra a tecnologia da informação. Decorre, pois, do Direito Informático, que é o conjunto de princípios, normas e entendimentos jurídicos oriundos da atividade informática. Assim, é um ato típico e antijurídico, cometido através da informática em geral, ou contra um sistema, dispositivo informática ou rede de computadores. Em verdade, pode-se afirmar que, no crime informática, a informática ou é o bem ofendido ou o meio para a ofensa a bens já protegidos pelo Direito Penal.[7]

Da mesma forma, Fabrício Roza (2007), apud. Damásio Jesus[8], destaca o pensamento de Klaus Tiedemann conceituando a criminalidade informática como todos os comportamentos ilegais ou prejudiciais à sociedade que envolvem a utilização de um computador. Necessário abordar que a expressão “computador” deve ser entendida como qualquer meio tecnológico.

---

[4] BOMFATI, Claúdio Adriano; KOLBE JUNIOR, Armando. **Crimes cibernéticos.** Ed. 1. Curitiba: Intersaberes, 2020. p. 62

[5] BOMFATI, Claúdio Adriano; KOLBE JUNIOR, Armando. **Crimes cibernéticos.** Ed. 1. Curitiba: Intersaberes, 2020. p. 62

[6] MARTINS, Dheneb. **Investigação Cibernética**. Ed. 1. Curitiba: Contentus, 2020. p. 23

[7] JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016, p. 49

[8] JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016, p. 48

No mesmo parágrafo, ainda, é importante frisar que o autor Damásio Jesus destaca o seguinte pensamento de Fabrício Roza:

> Kohn utiliza computer criminals para designar seus praticantes. Jean Pradel e Cristian Feuliard referem-se a 'infrações cometidas por meio de computador'. Há ainda quem prefira a expressão 'crimes de computador', 'cybercrimes', 'computer crimes', 'computing crimes', 'delito informática', 'crimes virtuais', 'crimes eletrônicos' ou ainda 'crimes digitais', 'crimes cibernéticos', 'infocrimes', 'crimes perpetrados pela internet', denominações distintas, mas que, no fundo, acabam por significar basicamente a mesma coisa[9]

Isto posto, o presente estudo intenta analisar a investigação de cibercrimes, se utilizando do termo como sinônimo de crimes virtuais, crimes digitais ou crimes cibernéticos, assim como observado. A partir da análise da investigação de cibercrimes, pretende-se dar destaque para os crimes no meio digital que necessitam de provas de caráter transnacional, tendo em vista que estes envolvem a investigação em cooperação internacional. Por conseguinte, será analisada a investigação cibernética à luz da Convenção de Budapeste, da Lei Geral de Proteção de Dados Brasileira e da Lei do Marco Civil da Internet, possibilitando destacar a intrínseca relação entre a investigação cibernética e a requisição de dados. Por fim, pretende-se destacar o instrumento dos Acordos Bilaterais de Assistência Mútua, especificamente o acordo entre o Brasil e os Estados-Unidos, e a controvérsia evidenciada pela Ação Declaratória de Constitucionalidade n° 51, destacando o instrumento do *Cloud Act* como possível solução ao desafio enfrentado pelo Brasil.

Para o desenvolvimento da pesquisa, será utilizada a metodologia da pesquisa documental e bibliográfica qualitativa, propiciando um levantamento de dados, segundo a doutrina jurídica, artigos científicos, legislação, entre outros meios bibliográficos para a análise adequada da reflexão proposta.

1. AS PROVAS NA INVESTIGAÇÃO DE CIBERCRIMES

1.1. CONCEITOS INICIAIS

[9] JESUS, Damásio de; MILAGRE, José Antonio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016, p. 49

O conceito de prova se traduz, segundo o doutrinador Aury Lopes Jr.[10], como os meios pelos quais se fará uma reconstrução do fato passado, mais especificamente do crime. Sendo assim, as provas admitem a criação de condições a partir das quais se permite a construção do convencimento do julgador.

No mesmo sentido, o doutrinador Noberto Avena[11], traz o conceito de prova como um conjunto de elementos produzidos, seja por requerimento das partes, seja por determinação do juiz, que visam ao convencimento quanto ao ocorrido. Além do conceito de prova, o autor ressalta, que o ônus da prova depende da natureza da alegação. Desse modo, esclarece que a acusação deverá provar a existência do fato que buscou imputar, assim como a materialidade e autoria da conduta de forma fundamentada, provando os fatos constitutivos da pretensão punitiva. Por outro lado, à defesa será imputado o ônus probatório de eventuais fatos extintivos, impeditivos ou modificativos da pretensão punitiva[12]. Diante disso, preconiza o artigo 156, *caput,* do Código de Processo Penal "A prova da alegação incumbirá a quem a fizer"[13].

O Direito Processual Penal Brasileiro adota o sistema de livre convencimento, consolidando o entendimento de que a prova visa ao convencimento do magistrado acerca da situação a ser examinada. Dessa forma, é delimitado no art. 155 do CPP: "o juiz formará sua convicção pela livre apreciação da prova produzida em contraditório judicial, não podendo fundamentar sua decisão exclusivamente nos elementos informativos colhidos na investigação, ressalvadas as provas cautelares, não repetíveis e antecipadas"[14].

Dado o exposto, o conceito de meios de prova pode ser definido, conforme explicita Guilherme de Souza Nucci[15], como os recursos lícitos, diretos ou indiretos, produzidos na investigação processual penal, que serão levados em conta pelo juiz. Sendo assim, podem ser traduzidos como os possíveis caminhos para se chegar à verdade real ao final do processo.

No contexto dos cibercrimes, as provas são, por consequência da matéria ou meio de concretização, digitais. Diante disso, não se constatam na legislação brasileira quaisquer óbices

---

[10] LOPES JR, Aury. **Direito processual penal**. São Paulo: Saraiva, 2020. 17, 2020, p. 383
[11] AVENA, Noberto, **Processo Penal.** Rio de Janeiro: Método, 2020. 12, rev., atual., ampl., p.492
[12] AVENA, Noberto, **Processo Penal.** Rio de Janeiro: Método, 2020. 12, rev., atual., ampl., p.502
[13] BRASIL. **Decreto-Lei Nº 3.689**, 3 de outubro de 1941. Código de Processo Penal, 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm. Acesso em: 16/04/2021
[14] BRASIL. **Decreto-Lei Nº 3.689**, 3 de outubro de 1941. Código de Processo Penal, 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm. Acesso em: 16/04/2021
[15] NUCCI, Guilherme de Souza. **Manual de Processo Penal.** Rio de Janeiro: Forense, 2021. 2, rev., atual., ampl., p. 260

quanto ao fato da prova se constituir no âmbito digital. De fato, o Código Civil, em seu art. 225, preleciona que "As reproduções fotográficas, cinematográficas, os registros fonográficos e, em geral, quaisquer outras reproduções mecânicas ou eletrônicas de fatos ou de coisas fazem prova plena destes, se a parte, contra quem forem exibidos, não lhes impugnar a exatidão"[16].

Além disso, o Código de Processo Civil (CPC) estabelece, em seu art. 369: "As partes têm o direito de empregar todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, para provar a verdade dos fatos em que se funda o pedido ou a defesa e influir eficazmente na convicção do juiz"[17]. Logo em seguida, no artigo 422 do CPC, é estabelecido que reproduções mecânicas, tais como fotografias, cinematografias, fonografias, entre outras, podem servir de prova se sua conformidade com o documento original não foi refutada pela parte contrária. De modo igual, o parágrafo primeiro estabelece: "§ 1º As fotografias digitais e as extraídas da rede mundial de computadores fazem prova das imagens que reproduzem, devendo, se impugnadas, ser apresentada a respectiva autenticação eletrônica ou, não sendo possível, realizada perícia"[18].

Ainda, devem ser observados os art. 439 a 441 do Código de Processo Civil que instituem que o uso de documentos eletrônicos depende da conversão à forma impressa e da verificação de autenticidade na forma estabelecida por lei. Não sendo esse convertido em forma impressa, ainda assim, poderá o juiz apreciar seu valor probante. Portanto, a legislação processual civil aceita amplamente os documentos eletrônicos, desde que sejam produzidos e conservados na forma da lei específica, conforme indica o art. 441 do CPC[19].

No âmbito penal, o Código de Processo Penal estabelece, em seu art. 231: "Salvo os casos expressos em lei, as partes poderão apresentar documentos em qualquer fase do processo.", c/c ao art. 232, parágrafo único "À fotografia do documento, devidamente autenticada, se dará o mesmo valor do original."[20]. Dessa forma, as legislações de regência aceitam como prova aquelas derivadas do âmbito digital, estabelecendo um consenso acerca da utilização desse meio de prova.

---

[16] BRASIL. **Lei Nº 10.406**, 10 de janeiro de 2002. Código Civil, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 16/04/2021

[17] BRASIL. **Lei N° 13.105**, de 16 de março de 2015. Código de Processo Civil, 2015. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 16/04/2021

[18] BRASIL. **Lei N° 13.105**, de 16 de março de 2015. Código de Processo Civil, 2015. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 16/04/2021

[19] BRASIL. **Lei N° 13.105**, de 16 de março de 2015. Código de Processo Civil, 2015. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 16/04/2021

[20] BRASIL. **Decreto-Lei Nº 3.689**, 3 de outubro de 1941. Código de Processo Penal, 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm. Acesso em: 16/04/2021

Além do abordado, a Lei 12.682 de 2012, que dispõe sobre a elaboração e arquivamento de documentos em meios eletromagnéticos, estabelece em seu art. 1°, parágrafo único, o conceito de digitalização: "Entende-se por digitalização a conversão da fiel imagem de um documento para código digital."[21]. A referida lei, traz, ainda, em seu art. 3°, a disposição de que o processo de digitalização deverá seguir os princípios da integridade, da autenticidade e, se necessário, da confidencialidade do documento digital, submetendo-se ao certificado digital emitido pela Infraestrutura de Chaves Públicas Brasileira - ICP – Brasil.

Por fim, ressaltando a prova digital no ordenamento jurídico, destaca-se a Lei do Processo Eletrônico, que dispõe sobre a informatização do processo judicial. Essa, por sua vez, admite amplamente a tramitação do processo pelo meio digital, dispondo, inclusive, em seu art. 11, que quaisquer documentos eletrônicos juntados ao processo com garantia da origem e do signatário, na forma da lei, serão reconhecidos como se originais fossem frisando ainda, em seu parágrafo primeiro, que terão a mesma força probante dos originais, salvo alegações motivadas e fundamentadas de adulteração[22].

1.2. EVIDÊNCIAS DIGITAIS

Dado o exposto, observa-se que as provas digitais são amplamente aceitas e amparadas pelo ordenamento jurídico brasileiro, contudo, no âmbito digital, algumas peculiaridades relacionadas à velocidade da criação, ampla difusão de informações e anonimato propiciado pela *Internet* são observadas, salientando dificuldades no processo investigativo cibernético.

Segundo o perito criminal Márcio Caneiro[23], quando se aborda o âmbito dos crimes cibernéticos, os vestígios deixados, os quais suportam a investigação, são vestígios digitais, tornando-se, portanto, evidências, para a comprovação de materialidade e autoria[24]. Complementando esse conceito, a autora Patrícia Peck[25] discorre sobre a evidência digital, conceituando-a como "toda informação ou assunto de criação, intervenção humana ou não que pode ser extraído de um compilado ou depositário eletrônico".

---

[21] BRASIL. **Lei N° 12.682**, de 9 de julho de 2012. Elaboração e arquivamento de documentos em meios eletromagnéticos, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12682.htm. Acesso em: 16/04/2021

[22] BRASIL. **Lei N° 11.419**, de 19 de dezembro de 2006. Lei do Processo Eletrônico, 2006. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11419.htm. Acesso em: 16/04/2021

[23] BRASIL. Tribunal Regional Federal da 3ª Região. Escola de Magistrados **Investigação e prova nos crimes cibernéticos**. São Paulo: EMAG, 2017, p. 37.

[24] BRASIL. Tribunal Regional Federal da 3ª Região. Escola de Magistrados **Investigação e prova nos crimes cibernéticos**. São Paulo: EMAG, 2017, p. 37.

[25] PECK, Patricia. **Direito digital.** São Paulo: Saraiva Educação, 2016. 6, p. 263.

Nesse sentido, nos crimes cibernéticos, para que se obtenham as informações para coleta de provas, faz-se necessário observar os registros cadastrais dos usuários por meio do *Internet Protocol* (IP), conceituado pelo Ministério Público Federal (MPF) da seguinte maneira:

> Quando o usuário faz a conexão à rede, recebe um número – o Internet Protocol (IP) já referido. Esse número, durante o tempo de conexão, pertence exclusivamente ao usuário, pois é graças a ele que o internauta pode ser "encontrado" na rede. A identificação do IP é o primeiro e mais importante passo para a investigação de um crime cibernético, como veremos adiante. Convém, desde logo, lembrar que o investigador deve ainda identificar a hora exata da conexão e o fuso horário do sistema, pois um número IP pertence ao usuário apenas durante o período em que ele está conectado; depois, o número é atribuído a outro internauta, aleatoriamente.[26]

Além disso, o MPF destaca que, as organizações que possuem domínio na *internet*, por meio do Sistema de Nome de Domínios (DNS)[27] gerenciam estes, decidindo sobre os nomes dos *hosts* e subdomínios[28]. Sendo assim, o ponto emissor onde se identifica o IP, pode estar em um domicílio, domínio público ou local de trabalho. Portanto, para a adequada investigação, deve ser feito um requerimento aos provedores que hospedam a página solicitando que estes forneçam os elementos necessários para a investigação, tais como os dados telemáticos.

Dessa maneira, o caminho a ser seguido para requisição de provas necessita de um conhecimento específico e especializado acerca dos meios de obtenção, além da cooperação dos provedores para fornecimento dos dados necessários. Logo, a investigação cibernética se torna ardilosa, na medida em que depende da colaboração do provedor para coletar as evidências digitais necessárias, que por sua vez, estão sujeitas à fragilidade, podendo ser mascaradas ou alteradas com outras ferramentas digitais.

Em vista disso, o MPF destaca algumas características das evidências digitais a serem observadas: a alta volatilidade, visto que podem ser manipuladas e alteradas para ocultar rastros; a facilidade em duplicar a evidência, permitindo uma comparação; a intangibilidade, dessa forma, não estão sujeitas facilmente à destruição; a relevância, visto que propiciam uma quantidade de informações de autoria essenciais para identificação do criminoso; a abundância,

---

[26] BRASIL, Ministério Público Federal, **Crimes Cibernéticos:** manual prático de investigação, 2006, p. 8.
[27] É por meio do DNS que se traduz o número IP.
[28] BRASIL. Ministério Público Federal**. Roteiro de atuação**: crimes cibernéticos. 2 ed. rev. - Brasília: MPF/2ªCCR, 2013, p. 39

necessitando de uma manipulação especializada, com filtragem das informações a serem utilizadas[29].

1.3. PERÍCIA DIGITAL

Pela natureza das evidências digitais e pelas características destacadas acima, faz-se necessário um tipo especializado de perícia – a perícia digital – também denominada de forense computacional. A perícia digital, portanto, busca extrair as informações deixadas digitalmente para que haja a correta apuração do crime cibernético praticado.

Segundo Caio César Lima, a perícia digital abrange desde a colheita das informações até o exame dos dados obtidos digitalmente, servindo como meio de prova no processo judicial penal[30]. No mesmo sentido, Felipe Caiado e Marcelo Caiado, apud Farmer e Venema, conceituam a perícia digital como a preservação, aquisição, análise, descoberta, documentação e apresentação das evidências digitais, com intuito de apurar o fato criminoso[31].

Faz-se necessário explicitar que, existem padrões metodológicos definidos para a correta coleta de evidências digitais. Atualmente, o Brasil visa se adequar aos parâmetros estabelecidos pela entidade norte-americana *Scientific Working Group on Digital Evidence* (SWGDE)[32]. Segundo essa, a coleta de evidências digitais estabelecidos pelo RFC 3227, deve ser feita de forma que a evidência precisa ser: admissível, em conformidade com as leis; autentica, possível de ligar-se ao crime investigado; completa, contando o fato como um todo e não apenas de uma perspectiva particular; confiável, de modo que a coleta e o armazenamento não permitam dúvidas sobre sua autenticidade e veracidade; convincente, podendo ser compreendida e creditada perante o julgamento[33].

---

[29] BRASIL. Ministério Público Federal**. Roteiro de atuação**: crimes cibernéticos. 2 ed. rev. - Brasília: MPF/2ªCCR, 2013, p. 172-173

[30] LIMA, Caio César Carvalho, **Aspectos legais da Perícia Forense Computacional em um cenário de Cloud Computing,** In: PROCEEDING OF THE FIFTH INTERNATIONAL CONFERENCE ON FORENSIC COMPUTER SCIENCE. Brasília: ICoFCS 2010 ABEAT (ed.), 2010, p. 25.

[31] CAIADO, Felipe B., CAIADO, Marcelo, **Combate à pornografia infantojuvenil com aperfeiçoamentos na identificação de suspeitos e na detecção de arquivos de interesse,** Crimes cibernéticos: coletânea de artigos: Brasília: MPF, 2018, p. 11

[32] TEIXEIRA, Tarcisio, **Direito digital e processo eletrônico**,5. ed., São Paulo: Saraiva Educação, 2020, p. 270

[33] Internet FAQ Archives. **Guidelines for Evidence Collection and Archiving**: RFC 3227. Disponível em: http://www.faqs.org/rfcs/rfc3227.html. Acesso em: 16/04/2021

Dessa forma, a perícia digital segue quatro fases para enfim se realizar o laudo pericial, sendo estas: a obtenção e coleta de dados; a identificação dos indícios; a preservação das provas; e a análise pericial[34].

Na fase de obtenção e coleta de dados, mantendo o processo legal, deve-se obter um mandado de busca e apreensão. Nesse contexto, busca-se obter os vestígios digitais a partir dos dados já detidos acerca do número de endereço IP, e outros possíveis identificadores do autor do delito para que haja a adequada execução do mandado[35]. Quando em âmbito de crimes computacionais, Tarcisio Teixeira, esclarece que as normas SWGDE classificam as provas em: provas digitais, aquelas armazenadas e transmitidas por meio digital; os dados objetos, que seriam objetos necessários ao processo; e os itens físicos, que se traduzem pelas mídias física que contém informações digitais, à exemplo de HDs, entre outros. Desse modo, por meio dessas provas se obtêm os dados, que podem se encontrar acessíveis, danificados ou ocultados no momento[36].

Em seguida, tem-se a fase de identificação de indícios, na qual busca-se identificar em quais indícios deve o perito focar, separando os essenciais, que se relacionam ao crime cibernético investigado. Faz-se possível, portanto, aqui, identificar a origem dos dados e obter informações sobre o fato ocorrido, de acordo com sua especificidade[37].

Quando na preservação das provas, observa-se o local ou maneira em que o crime foi cometido. Em vista disso, segue-se uma cadeia de custódia, assim como no processo penal quando com crimes são cometidos fisicamente. Se observa, então: a documentação das provas, a coleta e o armazenamento, o manuseio, e a proteção dos dados extraídos. Nesse âmbito, o doutrinador Tarcisio Teixeira explicita a necessidade de se obterem cópias dos dados que devem ser preservados em uma mídia virgem, livre de qualquer vírus e defeitos que possam comprometer a evidência para que haja uma maior segurança no processo[38].

Por fim, na análise pericial, observa-se a legitimidade da prova, definindo um limite à área de atuação de perito computacional, para que não contamine a coleta da prova por

---

[34] TEIXEIRA, Tarcisio, **Direito digital e processo eletrônico**,5. ed., São Paulo: Saraiva Educação, 2020, p. 270
[35] CANEIRO, Márcio Rodrigo de Freitas, **Perícia de informática nos crimes cibernéticos**, Tribunal Regional Federal da 3ª Região. Escola de Magistrados Investigação e prova nos crimes cibernéticos. São Paulo: EMAG, 2017, p. 37-39.
[36] TEIXEIRA, Tarcisio, **Direito digital e processo eletrônico**,5. ed., São Paulo: Saraiva Educação, 2020, p.270
[37] TEIXEIRA, Tarcisio, **Direito digital e processo eletrônico**,5. ed., São Paulo: Saraiva Educação, 2020, p.271
[38] TEIXEIRA, Tarcisio, **Direito digital e processo eletrônico**,5. ed., São Paulo: Saraiva Educação, 2020, p. 271

violações aos dados pessoais de indivíduos não envolvidos na investigação. Nesse sentido, o autor explicita que:

> Na análise das provas digitais, são utilizadas ferramentas que auxiliem o desenvolvimento pericial, bem como para obter a veracidade dos fatos. Estas ferramentas são *softwares* específicos para este fim ou *kits* completos e robustos, sendo definidas pelo profissional que realizará a análise. É o perito digital que no momento saberá qual é a mais adequada para cada caso. Podem ser empregadas ferramentas para recuperação de dados, análise de memória, análise de dados de uma rede, entre muitas outras ferramentas digitais.[39]

Ao passar por todas as fases, chega-se à coleta adequada dos dados e à elaboração do laudo pericial, que retrata, a partir das evidências digitais coletadas, os fatos observados, sem qualquer juízo de mérito, servindo apenas de embasamento para a ação judicial[40].

1.4. DESAFIOS DA PERÍCIA DIGITAL E O *CLOUD COMPUTING*

Dadas as características da prova digital e pela natureza da *internet*, por diversas vezes faz-se necessário requisitar dados a provedores estrangeiros, realçando o caráter transnacional da prova digital. À vista disso, Bechara (2011, apud. Domingos, Röder, 2018) explicita que a prova transnacional é aquela que se encontra em Estado distinto ao da autoridade judicial competente, ou quando os meios de provas se situam em Estados diversos, necessitando, portanto, da cooperação e auxílio para a obtenção destas[41].

Nesse contexto de transnacionalidade, surge a Computação em Nuvem *(Cloud Computing)*, que representa a possibilidade do armazenamento e acesso de dados, informações, entre outros, por meio de uma comunicação de redes, não envolvendo a necessidade de averiguação na própria máquina da qual proveio a infração delituosa. Dessa forma, para a investigação cibernética é conveniente aliar a perícia digital ao *Cloud Computing*, visto que os dados dos infratores podem estar localizados em *data centers* armazenados fora da jurisdição brasileira[42].

Nesse sentido, Caio César Lima ressalta que:

---

[39] TEIXEIRA, Tarcisio, **Direito digital e processo eletrônico**,5. ed., São Paulo: Saraiva Educação, 2020, p.271
[40] *Ibidem*, p. 272
[41]DOMINGOS, Fernanda Teixeira Souza; RÖDER, Priscila Costa Schereiner, **Obtenção de provas digitais e jurisdição na internet**, Ministério Público Federal. Câmara de Coordenação e Revisão, 2. Crimes cibernéticos, 2ª Câmara de Coordenação e Revisão, Criminal, Brasília: MPF, 2018, p. 30-31
[42] LIMA, Caio César Carvalho, **Aspectos legais da Perícia Forense Computacional em um cenário de Cloud Computing,** In: PROCEEDING OF THE FIFTH INTERNATIONAL CONFERENCE ON FORENSIC COMPUTER SCIENCE. Brasília: ICoFCS 2010 ABEAT (ed.), 2010, p.24

> Isto é, como acima já referido, não se precisará gravar os dados e informações comumente consultados na máquina utilizada, já que eles estarão na "nuvem", podendo ser acessados, de qualquer lugar do mundo, através de um computador, celular ou televisão com conexão à Internet. Essas informações estarão armazenadas em datas centers, poderosas centrais de processamento de dados, estando pouco ou quase nada no equipamento.[43]

Na realização da perícia digital na nuvem, portanto, faz-se possível a obtenção dos dados de forma ágil, sem necessidade de acesso físico aos dispositivos envolvidos. Contudo, a mesma característica torna o acesso dificultoso, uma vez que, por conta da estrutura da nuvem, os procedimentos devem ser específicos e a coleta de evidências se torna conflituosa, observada as questões jurídicas envolvendo o controle dos dados, além da distribuição geográfica. Dessa forma, a perícia digital tem sido reestruturada, originando o termo *Cloud Forensics*, o qual trata da investigação forense digital no *Cloud Computing*[44].

Destaca-se que se fazem presentes quatro modelos de implantação do *Cloud Computing*, sendo estes: em nuvem privada, que é administrada pela empresa ou terceiros; em nuvem pública, disponibilizada publicamente, observando o compartilhamento e limites segundo as políticas de segurança, inclusive os *Serviçe Legal Agreements* (SLA); em nuvem comunitária, que trata do compartilhamento em uma única nuvem por várias empresas, podendo ser administrada por uma empresa específica ou terceiros; e em nuvem híbrida, que trata de um modelo compostos por dois ou mais modelos dentre os explicitados[45].

Ruan et al. (2011, apud. Didoné, 2011)[46] propõem uma caracterização tridimensional dos desafios da perícia digital em nuvem, dividindo entre dimensão técnica, organizacional e jurídica. No âmbito jurídico, destacam-se alguns aspectos legais dessa nova modalidade da perícia digital. Observado que se trata de um âmbito altamente volátil, de compartilhamento amplo sem restrições de jurisdições, impõe-se a necessidade de forças internacionais e nacionais atuarem conjuntamente para garantir que o processo de perícia seja feito adequadamente, conforme as legislações de privacidade de dados. Da mesma forma, os autores ressaltam a necessidade da observância dos acordos de nível de serviço, denominados *Serviçe*

---

[43] *Ibidem*, p. 27

[44] ROMANOSKI, Vanderlei et al. **Forense computacional e a garantia das evidências no uso da computação em nuvem numa organização**. Gestão da Segurança da Informação-Unisul Virtual, 2019, p. 3-5

[45] TEIXEIRA, Tarcisio, **Direito digital e processo eletrônico**,5. ed., São Paulo: Saraiva Educação, 2020, p. 322-323

[46] DIDONÉ, Dener; José Guerra Barreto de Queiroz, Ruy. **Computação em nuvem: desafios e oportunidades para a forense computacional.** 2011. 112 f. Dissertação (Mestrado). Programa de Pós-Graduação em Ciência da Computação, Universidade Federal de Pernambuco, Recife, 2011, p.17

Legal Agreements (SLA), entre os provedores de serviço de nuvem (CSP) e os clientes, visto que estes estabelecem os serviços e as técnicas, além de impor limites e garantias ao usuário acerca das investigações forenses[47].

No mesmo sentido, o autor Vanderlei Romanoski informa que cada organização que consume os serviços fornecidos pela nuvem, define sua política de controle de acesso, assim como os fornecedores, promovendo um sistema de segurança e privacidade de dados dos usuários[48]. Conjuntamente às legislações de proteção de dados, a investigação deve se atentar às políticas de segurança dos acordos estabelecidos, assim como a política de segurança dos provedores. Nesse âmbito, Didoné ressalta a importância de definir procedimentos adequados à estrutura da nuvem, além de incentivos à colaboração entre as partes dos SLAs e a polícia durante a investigação[49].

2. ANÁLISE À LUZ DA LEGISLAÇÃO BRASILEIRA

2.1. A CONVENÇÃO DE BUDAPESTE

A Convenção de Budapeste, também denominada Convenção sobre o Cibercrime, de 2001, com entrada em vigor em 2004, é o primeiro tratado internacional acerca dos cibercrimes. Visando estabelecer uma política criminal comum para proteção contra os ataques digitais por meio de uma legislação, ressaltou a importância da cooperação internacional para enfrentar o novo paradigma digital.

Em 2021, o tratado conta com 47 países membros do Conselho Europeu e 31 países não membros, com o total de 66 países que ratificaram a convenção. Destaca-se que o Brasil foi convidado, em dezembro de 2019, a aderir ao referido tratado, tendo o convite validade de 3

[47] DIDONÉ, Dener; José Guerra Barreto de Queiroz, Ruy. **Computação em nuvem: desafios e oportunidades para a forense computacional.** 2011. 112 f. Dissertação (Mestrado). Programa de Pós-Graduação em Ciência da Computação, Universidade Federal de Pernambuco, Recife, 2011, p.17

[48] ROMANOSKI, Vanderlei et al. **Forense computacional e a garantia das evidências no uso da computação em nuvem numa organização**. Curso de Especialização em Gestão da Segurança da Informação-Unisul Virtual, 2019, p.15

[49] DIDONÉ, Dener; José Guerra Barreto de Queiroz, Ruy. **Computação em nuvem: desafios e oportunidades para a forense computacional.** 2011. 112 f. Dissertação (Mestrado). Programa de Pós-Graduação em Ciência da Computação, Universidade Federal de Pernambuco, Recife, 2011, p.61

anos. Logo após, o texto foi enviado ao Congresso Nacional para as devidas considerações com fins de adesão[50].

O tratado conta com 4 capítulos: terminologia; medidas a tomar a nível nacional; cooperação internacional; e disposições finais.

Para fins de compreensão dos conceitos traz-se a seguir as definições utilizadas. A Convenção trata como dados informáticos todos os fatos, informações ou conceitos que são processados em um sistema de computadores ou programas. Da mesma forma, o fornecedor de serviço é conceituado como qualquer entidade que faculte o uso dos seus serviços e comunicação por sistema informático, ou entidade que processe ou armazene dados informáticos do serviço de comunicação ou dos usuários desse serviço. Por fim, a Convenção aborda os dados de tráfego, que seriam os dados informáticos que se comunicam por um sistema informático, como um elemento de uma cadeia de comunicação, indicando, por sua vez, a origem, o destino, o trajeto, hora, data, tamanho, duração e tipo de serviço[51].

A Seção 2 do referido tratado, título 4, artigo 19, parágrafo 3°, salienta que as partes adotarão as respectivas medidas legislativas para:

> a) apreender ou obter de forma semelhante um sistema informático ou uma parte deste ou um suporte de armazenamento informático;
> b) realizar e conservar uma cópia desses dados informáticos;
> c) preservar a integridades dos dados informáticos pertinentes armazenados;
> d) tornar inacessíveis ou eliminar esses dados do sistema informático acedido[52]

Conforme estabelece o Relatório Explicativo da Convenção de Budapeste, no ponto 197[53], o termo “apreender”, usado no tratado, inclui o transporte do suporte físico com os dados ou informações, e, abrange ainda, os programas necessários para se obter acesso. Por sua vez, o termo da “guarda” se refere aos meios possíveis de manipular os dados. Dessa forma, a

---

[50] Brasil é convidado a aderir à Convenção do Conselho da Europa contra a Criminalidade Cibernética. **Secretaria-Geral**. Presidência da República. Notícias, julho 2020, 24/07/2020. Disponível em: https://www.gov.br/secretariageral/pt-br/noticias/2020/julho/brasil-e-convidado-a-aderir-a-convencao-do-conselho-da-europa-contra-a-criminalidade-cibernetica. Acesso em: 14/05/21.

[51] COUNCIL OF EUROPE. **Convenção sobre o Cibercrime**. Budapest, 23.XI.2001. Acesso em: https://rm.coe.int/16802fa428 . Acesso em: 14/05/21

[52] COUNCIL OF EUROPE. **Convenção sobre o Cibercrime**. Budapest, 23.XI.2001. Acesso em: https://rm.coe.int/16802fa428 . Acesso em: 14/05/21

[53] COUNCIL OF EUROPE**. Relatório Explicativo da Convenção de Budapeste**, 23, XI,2001. Disponível em: https://rm.coe.int/16802fa429 Acesso em 14/05/21

Convenção trata tanto dos dados obtidos por meios tangíveis, como por meios intangíveis (acessíveis *on-line*)[54].

O presente estudo se debruça especificamente sobre o capítulo terceiro da Convenção, que discorre acerca da cooperação internacional, evidenciando o trânsito de dados entre países e a necessidade de se observarem padrões devido ao caráter volátil dos dados.

Adentrando a importância da requisição de dados no processo investigativo, o art. 29 apresenta a conservação dos dados informáticos armazenados, que deve ser feita por período não inferior a 60 dias, salientando que uma das partes pode demandar à outra os dados que se encontrem no território dessa última, apresentando um pedido de auxílio mútuo. Esse, por sua vez, deve especificar à autoridade que demanda, a infração objeto de investigação, os dados a conservar, o nexo causal, as informações que permitam identificar o autor do fato pelos dados informáticos ou sistema informático e a necessidade da conservação dos dados com pedido de acesso, apreensão ou obtenção dos referidos dados[55].

Ainda no campo da requisição de dados para investigação penal, o parágrafo 3° do referido artigo conceitua a criminalidade dupla, como sendo a constatação de que o crime observado no país requerente se encontra no ordenamento penal do país requerido. Nesse sentido, segundo o Relatório Explicativo, esse princípio deve ser relativizado, não devendo ser requisito necessário para o pedido de prévia conservação dos dados, tendo em vista que seria contraproducente, dada a volatilidade dos dados e o fato da medida de preservação dos dados não ser considerada intrusiva. Entretanto, caso a parte requerida estabeleça o princípio como condição e motivadamente acredite que este não será preenchido, pode se reservar no direito de recusar, ressalvados pela Convenção os seguintes delitos: contra sistemas informáticos; contra dados informáticos; relacionados com computadores ou com conteúdo e violações de direito autorais e conexos[56]. Ainda, o parágrafo 5° do mesmo artigo estabelece que a parte requerida

---

[54] DELGADO, Vladimir Chaves. **Cooperação internacional em matéria penal na convenção sobre o cibercrime.** 2007, 315 p. Dissertação (Mestrado em Direito das Relações Internacionais) – Centro Universitário de Brasília, Brasília, 2012. p. 190-195

[55] COUNCIL OF EUROPE. **Convenção sobre o Cibercrime**. Budapest, 23.XI.2001. Acesso em: https://rm.coe.int/16802fa428 . Acesso em: 17/05/21

[56] COUNCIL OF EUROPE. **Convenção sobre o Cibercrime**. Budapest, 23.XI.2001. Acesso em: https://rm.coe.int/16802fa428 . Acesso em: 17/05/21

poderá recusar o requerimento de preservação quando em face de prejuízo a sua soberania, segurança, ordem pública ou interesses essenciais, ou, em face de infrações políticas[57].

Acerca do local dos dados, o art. 30 estabelece que, ao executar o pedido de conservação dos dados informáticos, a parte requerida deverá informar ao requerente se ficar caracterizado que um fornecedor de serviços se situa em outro Estado, além de fornecer informações para a correta identificação do fornecedor. De igual maneira, são estabelecidas as possibilidades de recusa nos mesmos termos do artigo anterior. Por conseguinte, o art. 31 estabelece o auxílio entre os países para o acesso, investigação, apreensão ou obtenção de dados informáticos, por meio de um sistema informático, no território da parte requerida, fornecendo estes com agilidade quando presentes os motivos de vulnerabilidade dos dados e vigência de instrumentos de cooperação célere[58].

O presente tratado permitiu, de igual forma, elucidar o debate acerca da possibilidade no acesso de dados situados no território da parte requerida, sem permissão necessária (art. 32 da Convenção). Por ser um tema controverso, foram acolhidas duas hipóteses possíveis: dados em fontes abertas; e dados em um sistema informático quando com consentimento legal e voluntário da pessoa legal autorizada a divulgar[59]. Nesse âmbito, a Convenção buscou se utilizar dos mecanismos de interceptação de telecomunicações já adotados usualmente, porém de forma adaptada ao contexto do trânsito de dados, criando as medidas de coleta em tempo real de dados de tráfico e de interceptação de dados de conteúdo.

Portanto, o art. 33 do presente tratado, discorre sobre as peculiaridades dos cibercrimes, destacando a necessidade de se obterem os dados necessários em tempo real. Frisa-se que as partes poderão se reservar no direito de limitar a medida de fornecimento dos dados, assim como o âmbito de aplicação desta. Nesse sentido, o parágrafo do referido artigo estabelece que "Cada Parte concederá o auxílio pelo menos no que diz respeito às infrações penais relativamente às quais seria possível a recolha ao nível interno a recolha em tempo real dos dados de tráfego em caso semelhante"[60].

---

[57] COUNCIL OF EUROPE. **Convenção sobre o Cibercrime**. Budapest, 23.XI.2001. Acesso em: https://rm.coe.int/16802fa428 . Acesso em: 14/05/21

[58] *Ibidem*

[59] COUNCIL OF EUROPE. **Convenção sobre o Cibercrime.** Budapest, 23.XI.2001. Acesso em: https://rm.coe.int/16802fa428 . Acesso em: 17/05/21

[60] COUNCIL OF EUROPE. **Convenção sobre o Cibercrime**. Budapest, 23.XI.2001. Acesso em: https://rm.coe.int/16802fa428 . Acesso em: 17/05/21

No art. 34, por sua vez, é dado destaque às leis domésticas, estabelecendo que estas impõem limites ao auxílio mútuo no âmbito do recolhimento dos registros em tempo real em relação aos dados com o conteúdo de comunicações transmitidas por sistema informático. Aponta-se, portanto, a necessidade de as partes estabelecerem seus próprios parâmetros legais para a devida execução da medida de requisição[61].

Por fim, analisa-se o art. 35 da referida Convenção, em que se reforça, mais uma vez, a necessidade de uma intervenção rápida para obtenção dos dados por meio de uma rede informática entre as partes. A rede 24/7, denominada assim pelo fato de ficar disponível por 24 horas nos 7 dias da semana, seria estabelecida para fornecer um auxílio imediato nas investigações e processos penais relacionados aos dados e sistemas informáticos. Por conseguinte, as seguintes medidas são mencionadas no parágrafo primeiro:

> a) A prestação de aconselhamento técnico;
> b) A conservação de dados em conformidade com os artigos 29° e 30°, e
> c) A recolha de provas, informações de carácter jurídico e localização de suspeitos[62]

Dispõe-se, ainda, nos parágrafos segundo e terceiro, que o ponto de contato estabelecido pela rede 24/7 deverá ter capacidade técnica para responder à requerente, podendo agir em cooperação com outros órgãos ou entidades do sistema, sendo necessário possuir equipe especializada para o funcionamento da rede[63].

Dessa forma, a Convenção de Budapeste se relaciona diretamente com a investigação de cibercrimes, inovando com medidas para requisição, aquisição, preservação, entre outras ações relacionadas aos dados informáticos e sistemas informáticos, todavia, sem retirar a autonomia dos países assinantes de determinarem suas legislações internas para se adequarem às suas disposições, assim como da sua compatibilidade com os instrumentos de cooperação internacional.

---

[61] COUNCIL OF EUROPE. **Convenção sobre o Cibercrime**. Budapest, 23.XI.2001. Acesso em: https://rm.coe.int/16802fa428 . Acesso em: 17/05/21

[62] COUNCIL OF EUROPE. **Convenção sobre o Cibercrime**. Budapest, 23.XI.2001. Acesso em: https://rm.coe.int/16802fa428 . Acesso em: 17/05/21

[63] COUNCIL OF EUROPE. **Convenção sobre o Cibercrime**. Budapest, 23.XI.2001. Acesso em: https://rm.coe.int/16802fa428 . Acesso em: 17/05/21

2.2. LEI DO MARCO CIVIL DA *INTERNET* (LEI 12.965)

Pretendendo regular o uso da *internet* no Brasil, surge em 2014, a Lei do Marco Civil da Internet, sendo um marco de grande relevância no cenário brasileiro, tendo em vista que delimitou princípios, garantias, direitos e deveres aos usuários, frente à atuação estatal. Quando na elaboração do Projeto de Lei n° 2126/2011, a exposição de motivos demonstra que o intuito do projeto era preservar os direitos dos usuários, além de abrigar as responsabilidades dos provedores de acesso e de conteúdo quando na investigação de ilícitos penais.[64]

Nesse sentido, o art. 3° do Marco Civil da *Internet*, estabelece os princípios que delimitam a Lei:

> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei; IV - preservação e garantia da neutralidade de rede; V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas; VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei; VII - preservação da natureza participativa da rede; VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.[65].

Dessa forma, alguns conceitos essenciais foram destacados. O Marco Civil estipulou o conceito de endereço de protocolo de *internet* (IP) como sendo o código atribuído ao terminal de uma rede para identificação. Igualmente, o conceito de administrador de sistema autônomo, como sendo "a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País" (art. 5°, inc. IV da Lei do Marco Civil)[66]. Ainda, outros conceitos trazidos pela Lei 12.965, são: o registro de conexão, sendo o conjunto de informações da conexão efetuada, incluindo o endereço IP; e o conceito de registros de acesso a aplicações de *internet* como "o conjunto de

---

[64] ROCHA, Lilian Rose Lemos (coord.) et al. **Caderno de pós-graduação em direito**: Crimes Digitais. Brasília: UniCEUB: ICPD. 2020. p.126

[65] BRASIL. **Lei N° 12.965**, de 23 de abril de 2014. Marco Civil da Internet, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acesso em: 30/04/2021

[66] BRASIL. **Lei N° 12.965**, de 23 de abril de 2014. Marco Civil da Internet, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acesso em: 30/04/2021

informações referentes à data e hora de uso de uma determinada aplicação de *internet* a partir de um determinado endereço IP" (art. 5° Lei do Marco Civil)[67].

A partir dessas elucidações, acentua-se que há uma relação com a investigação dos cibercrimes, visto que as definições trazidas são partes essenciais para a perícia digital averiguar o ilícito penal. Adentrando na definição de registro de conexão, esta trata das informações detidas pelos provedores de acesso, sendo a pessoa jurídica que fornece o acesso à *internet* pelo seu serviço de banda larga, à exemplo da Claro, Net virtual etc. Quanto aos registros de acesso a aplicações de *internet*, os dados se encontram em posse dos provedores de aplicações de *internet*, conceituados pelo art. 15 da Lei do Marco Civil como pessoas jurídicas, de atividade organizada, profissional e com fins econômicos. Além disso, no art. 5°, inciso VII da referida Lei, as aplicações de *internet* são definidas pelas funcionalidades que podem ser acessadas por meio de um terminal[68].

O conceito de provedor de aplicação de *internet*, apelidado de PAI, ainda encontra óbices quanto à sua exata definição. Dessa forma, seguir-se-á o seguinte entendimento acerca do provedor de aplicação:

> aquele que utiliza a conexão de um ponto de acesso para disponibilizar serviços ao agente usuário da rede, podem ser caracterizados como pessoa jurídica, que exerça atividade de forma organizada e com fins econômicos ou ainda a pessoa natural ou jurídica que não preencha esses requisitos[69]

Adentrando no aspecto da requisição de dados para a investigação, o art. 10° do Marco Civil da Internet estabelece que os registros de conexão e de acesso a aplicações de *internet*, dados pessoais e os conteúdos de comunicações privadas devem ser preservados, à luz da intimidade, da vida privada, da honra e da imagem. Contudo, o parágrafo primeiro estabelece que o provedor responsável – aqui não diferenciando os provedores, dessa forma abrangendo os dois citados anteriormente – devem disponibilizar os registros mencionados de forma

---

[67] BRASIL. **Lei N° 12.965**, de 23 de abril de 2014. Marco Civil da Internet, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acesso em: 30/04/2021

[68] ROCHA, Lilian Rose Lemos (coord.) et al. **Caderno de pós-graduação em direito**: Crime Digitais. Brasília: UniCEUB: ICPD. 2020. p.127-128

[69] DE OLIVEIRA DOS SANTOS, Thiago; FERREIRA MONTENEGRO DUARTE, Bruno. A Responsabilidade Civil Dos Provedores De Aplicação De Internet No Tratamento De Dados À Luz Da Lei. No 12.965/2014 Denominada O Marco Civil Da Internet. **Revista Eletrônica de Direito da Faculdade Estácio do Pará**, [S.l.], v. 5, n. 7, p. 79 - 100, jun. 2018. ISSN 2359-3229, p.84 Disponível em: <http://revistasfap.com/ojs3/index.php/direito/article/view/193>. Acesso em: 30 abr. 2021.

autônoma, juntamente com os dados pessoais ou outras informações que possam identificar o usuário ou o terminal quando em face de ordem judicial, respeitados os direitos e garantias do usuário[70].

Ainda, o art. 11 da referida lei dispõe que, devem ser resguardados os direitos dos usuários e a proteção dos dados pessoais nas operações de coleta, armazenamento, guarda e tratamento dos registros, dados pessoais, e comunicações pelos provedores, ocorrendo pelo menos um dos atos em território brasileiro. Em relação à transnacionalidade do processo, o parágrafo segundo explicita que o disposto no art. 11, *caput*, se aplica "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"[71].

Necessário ressaltar que, os provedores de conexão à *internet* possuem o dever de manter os registros de conexão, sob sigilo, pelo prazo de 1 ano, podendo a autoridade policial, administrativa ou o Ministério Público requerer prazo superior. Além disso, ao requerer os dados, a autoridade tem o prazo de 60 dias do requerimento para ingressar com pedido de autorização judicial para acessar tais dados. Quanto aos provedores de aplicações de *internet*, o prazo para manter os registros de acesso a aplicação de *internet* é de 6 meses, também sujeitos à prorrogação do prazo por requisição das autoridades policiais, administrativas ou do Ministério Público[72]. Apesar do dever de manter os registros pelos períodos destacados, frisa-se que, conforme disposto no art. 14 da lei abordada, não poderão os provedores registrar e guardar as aplicações feitas na *internet* pelo usuário, ou seja, os conteúdos, mas tão somente os registros dos sites acessados[73].

Destaca-se, de igual maneira que a parte interessada poderá, para fazer prova em processo judicial cível ou penal, requerer ao juiz que ordene ao responsável pela guarda, o fornecimento de registros de conexão ou de registros de acesso a aplicações de *internet* (art. 22 da Lei do Marco Civil da Internet). O requerimento deve conter indícios fundados da prática do

---

[70] BRASIL. **Lei N° 12.965**, de 23 de abril de 2014. Marco Civil da Internet, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acesso em: 30/04/2021

[71] BRASIL. **Lei N° 12.965**, de 23 de abril de 2014. Marco Civil da Internet, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acesso em: 30/04/2021

[72] BRASIL. **Lei N° 12.965**, de 23 de abril de 2014. Marco Civil da Internet, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acesso em: 30/04/2021

[73] BRASIL. **Lei N° 12.965**, de 23 de abril de 2014. Marco Civil da Internet, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acesso em: 30/04/2021

ilícito, justificativa motivada de requisição dos registros e o período necessários dos registros a serem requisitados[74].

Necessário ainda, abordar o Decreto n° 8.771 de maio de 2016, que regulamenta a presente Lei do Marco Civil, tratando acerca da discriminação dos dados na *internet*, assim como dos procedimentos para guarda e proteção de dados. Nesse sentido, o decreto explana a exigência de neutralidade da rede, evidenciando a necessidade de um tratamento isonômico. Além disso, estabelece em seu art. 11 que para o pedido de acesso aos dados cadastrais (filiação, endereço, qualificação pessoal), devem ser indicados os fundamentos legais e a motivação deve ser específica, vedados os pedidos coletivos ou genéricos. Contudo, o provedor não fica obrigado a disponibilizar esses dados se informar que não os coleta (art. 11 §1° do Decreto 8.771)[75].

Observa-se, ainda, que é recomendado que os provedores de conexão e de aplicações retenham a menor quantidade possível de dados pessoais[76], comunicações privadas e registros, que serão excluídos assim que atingirem a finalidade ou encerrado o prazo determinado legalmente (art. 13 §2° Decreto 8.771), sempre respeitando o direito à confidencialidade (art. 16 do referido Decreto)[77].

Apesar da lei delimitar garantias e prazos em relação aos usuários e seus dados, permitindo que as possíveis investigações cibernéticas tenham uma certeza acerca dos registros pelo prazo delimitado, fazem-se presentes crescentes críticas acerca do caráter transnacional da *internet* que não foi acompanhado. Observada a prevalência da influência norte-americana, em relação à localização de entidades provedoras de aplicações de *internet*, gera-se, portanto, uma grande concentração de *data centers* nos Estados-Unidos, tais como *Lakeside Technology Center*, *Google*, *Apple*, etc., ressaltando a necessidade de haver uma requisição de dados internacional, principalmente quando o crime cibernético é cometido envolvendo diversas jurisdições, ou quando as empresas se utilizam de nuvens de fornecedores internacionais[78].

---

[74] BRASIL. **Lei N° 12.965**, de 23 de abril de 2014. Marco Civil da Internet, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acesso em: 30/04/2021.

[75] BRASIL. **Decreto N° 8.771**, de 11 de maio de 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8771.htm Acesso em: 07/05/2021

[76] Dados relacionados à pessoa natural identificada ou identificável

[77] BRASIL. **Decreto N° 8.771**, de 11 de maio de 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8771.htm Acesso em: 07/05/2021

[78] ASSOCIAÇÃO NACIONAL DOS PROCURADORES DA REPÚBLICA, **Proteção de dados pessoais e investigação criminal**, 3ª Câmara de Coordenação e Revisão. Ministério Público Federal e Organizadores:

Nesse sentido, a Lei do Marco Civil delimita a proteção ao usuário em um contexto de vazamento de dados de forma irregular, contudo, com o aumento progressivo de crimes cibernéticos, evidencia-se uma lacuna jurídica em relação aos aspectos propriamente penais da requisição de dados para a investigação digital e da requisição internacional de dados.

2.3. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

A Lei Geral de Proteção de Dados Pessoais (Lei n° 13.709, de 14 de agosto de 2018) é o resultado da pressão internacional, mais especificamente europeia, para o enfrentamento dos cibercrimes. Com a entrada em vigor do Regulamento Geral sobre a Proteção de Dados em 2018 pela União Europeia, e a Convenção de Budapeste de 2002, o Brasil, se espelhando nesse contexto, buscou legislar, igualmente, acerca do tratamento de dados.

Dessa forma, a lei traz alguns conceitos chaves para a compreensão adequada do estudo, sendo estes: os dados pessoais, ou seja, as informações relacionadas a pessoa natural; os dados sensíveis, relacionados à origem racial, étnica etc.; e os dados anonimizados, que impedem uma vinculação direta da informação com um titular. Da mesma maneira, é necessário distinguir o conceito de banco de dados, que se traduz pelo conjunto de dados pessoais, além da definição acerca do tratamento de dados que envolve qualquer operação realizada com os dados pessoais[79]. Outrossim, é salientado o conceito da transferência internacional de dados como sendo a transferência de dados pessoais para país estrangeiro ou organização internacional, se relacionando diretamente com o conceito de uso compartilhado de dados, definido como a transferência ou compartilhamento de bancos de dados entre órgãos ou entidades com autorização específica para tratamento (art. 5°, incisos I, II, III, IV, XV, XVI, da Lei. 13.709)[80].

A LGPD estabelece em seu bojo um escopo de atuação, destacando não se aplicar nas seguintes situações: dados relacionados à uma pessoa jurídica protegidos pela lei de propriedade intelectual; dados pessoais para fins particulares e não econômicos; tratamento de dados para fins jornalísticos, acadêmicos, artísticos; tratamento de dados para segurança pública, defesa

---

Vladimir Barros Aras, Andrey Borges de Mendonça, Walter Aranha Capanema, Carlos Bruno Ferreira da Silva e Marcos Antônio da Silva Costa. Brasília: ANPR, 2020, p. 517.

[79] BRASIL. **Lei N° 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 07/05/2021

[80] BRASIL. **Lei N° 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 07/05/2021

nacional, segurança do Estado, e com relação a infrações penais; e, por fim, dados em trânsito que não têm destino ao tratamento no Brasil (art. 4° da LGPD)[81].

Ainda acerca da aplicação, a LGPD é imposta às empresas que tenham estabelecimento no Brasil, oferecem serviços ao consumidor brasileiro, ou, coletam dados de indivíduos localizados no país. Ainda é constatada que pode haver uma aplicação extraterritorial para toda empresa que tiver filial no Brasil, oferecer serviços, ou coletar e tratar dados no território nacional (art. 3° da LGPD)[82].

Por outro lado, após expressamente denotar que a referida lei não se aplica ao tratamento de dados pessoais em atividades de investigação e repressão de infrações penais (art. 4°, inc. III, alínea d, da LGPD), o parágrafo primeiro do art. 4° preconiza que

> O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei[83]

Nesse âmbito, apesar da restrição acerca da aplicação legislativa, o art. 33, inc. I e II da LGPD preconiza a possibilidade de transferência internacional de dados pessoais para países ou organismos que proporcionem a adequada proteção dos dados no tratamento, garantindo os princípios e direitos do titular. Além disso, aborda a transferência de dados no caso específico da cooperação internacional entre órgãos públicos de inteligência, de investigação e de persecução, conforme instrumentos de direito internacional (art. 33, inc. III, da LGPD)[84].

Dessa forma, tem-se um embate na legislação analisada, visto que o art. 4°, inc. III, conforme mencionado, exclui do escopo da lei o tratamento de dados quando no âmbito da investigação penal, porém o art. 33, inc. III, ressalta a cooperação internacional de trânsito de

---

[81] BRASIL. **Lei N° 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 07/05/2021
[82] BRASIL. **Lei N° 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 07/05/2021
[83] *Ibidem*
[84] BRASIL. **Lei N° 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 07/05/2021

dados visando fins de persecução penal, possibilitando uma interpretação da aplicação da lei para infrações penais[85].

Não obstante, destaca-se, ainda que a LGPD menciona o futuro estabelecimento de legislação específica para o tratamento de dados no âmbito penal (art. 4, §1° da LGPD), cogitando-se, atualmente, a criação de uma nova lei de proteção de dados para persecução penal, observadas as discussões recentes na Câmara dos Deputados acerca da "LGPD penal", denominada popularmente[86].

Sendo assim, embora a Lei Geral de Proteção de Dados Pessoais possua disposição excluindo da sua competência o tratamento de dados para investigações penais, os dados usados para as investigações estariam, da mesma forma, sujeitos ao tratamento estabelecido por esta, uma vez que, quando ainda não requisitados no âmbito penal, estão abrangidos nas situações de escopo da lei. Dessa forma, o embate se relaciona ao uso desses dados no âmbito penal, fato a ser regulado ainda pelo ordenamento brasileiro.

3. COOPERAÇÃO INTERNACIONAL PARA REQUISIÇÃO DE DADOS

3.1. TRATADO DE ASSISTÊNCIA JURÍDICA MÚTUA[87] (MLAT)

Conforme explanado pelos capítulos anteriores, resta evidenciada a dificuldade de uma investigação cibernética, dadas as características das provas e as especificidades dos procedimentos de requisição. Além do citado, tem-se ainda, o debate sobre a jurisdição da prova, tendo em vista os ordenamentos jurídicos diversos com regras distintas acerca dos procedimentos e dos crimes. Dessa forma, são adotados instrumentos legais para que se faça possível a cooperação para o trânsito de dados entre países no âmbito penal.

Nesse sentido, observam-se os Acordos de Assistência Judiciária, ou do inglês *Mutual Legal Assistance Treaties* (MLATs), como instrumentos cooperativos para se obter as devidas

---

[85] BRASIL. **Lei N° 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 07/05/2021

[86] ASSOCIAÇÃO NACIONAL DOS PROCURADORES DA REPÚBLICA, **Proteção de dados pessoais e investigação criminal**, 3ª Câmara de Coordenação e Revisão. Ministério Público Federal e Organizadores: Vladimir Barros Aras, Andrey Borges de Mendonça, Walter Aranha Capanema, Carlos Bruno Ferreira da Silva e Marcos Antônio da Silva Costa. Brasília: ANPR, 2020. p. 148

[87] Tradução livre

provas de acordo com as legislações de cada parte. Conforme destacam Guilherme Guidi e Francisco Rezek, os MLATs consistem em instrumentos de padronização de procedimentos para que a cooperação possa atender ambos os procedimentos legais das partes, permitindo uma compatibilidade e eliminando dificuldades e ilegalidades para a requisição[88].

Portanto, é necessário salientar o MLAT entre o Brasil e os Estados-Unidos, na medida em que os Estados-Unidos representam um grande *data center* mundial, sendo essencial a cooperação para obtenção de dados juntos aos provedores situados no país.

3.1.1. MLAT – Brasil e Estados Unidos

O MLAT, estabelecido entre o Brasil e os Estados Unidos, foi celebrado em 14 de outubro de 1997, entrando em vigor em 2001. O acordo abrange o desejo de "facilitar a execução das tarefas das autoridades responsáveis pelo cumprimento da lei de ambos os países, na investigação, inquérito, ação penal e prevenção do crime por meio de cooperação e assistência judiciária mútua em matéria penal"[89].

Dessa forma, prevê em seu bojo a assistência em várias áreas e procedimentos investigativos, tais como:

> tomada de depoimentos ou declarações de pessoas; b) fornecimento de documentos, registros e bens; c) localização ou identificação de pessoas (físicas ou jurídicas) ou bens; d) entrega de documentos; e) transferência de pessoas sob custódia para prestar depoimento ou outros fins; f) execução de pedidos de busca e apreensão; g) assistência em procedimentos relacionados a imobilização e confisco de bens, restituição, cobrança de multas; e h) qualquer outra forma de assistência não proibida pelas leis do Estado Requerido.[90]

---

[88] GUIDI, Guilherme Berti de Campos; REZEK, Francisco. **Crimes na internet e cooperação internacional em matéria penal entre Brasil e Estados Unidos**. Rev. Bras. Polít. Públicas, Brasília, v. 8, nº 1, 2018 p.276-288, p. 284.

[89] BRASIL. **Decreto N° 3.810**, de 2 de maio de 2001, Acordo de Assistência Judiciária em Matéria Penal entre Brasil e Estados Unidos. Disponível em http://www.planalto.gov.br/ccivil_03/decreto/2001/D3810.htm Acesso em: 21/05/2021

[90] BRASIL. **Artigo I, ponto 2 do Decreto N° 3.810**, de 2 de maio de 2001, Acordo de Assistência Judiciária em Matéria Penal entre Brasil e Estados Unidos. Disponível em http://www.planalto.gov.br/ccivil_03/decreto/2001/D3810.htm Acesso em: 21/05/2021, Art. I, parágrafo 2, do Decreto 3.810.

Se trata, então, de um instrumento celebrado visando um contexto de provas tangíveis. Contudo, conforme se observou, com as recentes transformações tecnológicas, outra realidade digital surge e adaptações são imprescindíveis.

As solicitações são fornecidas e recebidas pelas autoridades centrais de cada parte, no Brasil, o Ministério da Justiça, por meio do Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional, e nos Estado Unidos, o Procurador-Geral ou pessoa que este designe, dentro do Departamento de Justiça americano. A solicitação é feita por escrito, sob diversas formalidades, dependendo de motivação específica do pedido[91].

No âmbito dos cibercrimes, ressaltam-se dois procedimentos principais observados pelo MLAT e dispostos nos artigos XIII e XIV, que tratam da entrega de documentos e busca e apreensão[92]. O artigo XIII prevê que a entrega de documento deve ser feita observando os dispositivos do acordo e de forma a cumprir o pedido ao máximo. Também é disposto que, se for necessário o comparecimento de uma pessoa perante a autoridade do requerente, deve haver um pedido com antecedência. O artigo XIV, por sua vez, trazendo as disposições da busca e apreensão, aborda que o pedido para o mandado de busca, apreensão e entrega deve ser motivado, justificando a ação segundo as leis do Estado Requerido. Ainda é disposto que a Autoridade Central do Requerido poderá requerer termos ou condições para proteção de interesses quando na transferência do bem[93].

Ressalta-se que o presente instrumento prevê que a requisição de busca e apreensão deve ser motivada segundo a legislação norte-americana, visto que é estabelecido que deve seguir a legislação do Estado Requerido. Portanto, é estabelecido no art. V, item 3:

> As solicitações serão executadas de acordo com as leis do Estado Requerido, a menos que os termos deste Acordo disponham de outra forma. O método de

[91] GUIDI, Guilherme Berti de Campos; REZEK, Francisco. **Crimes na internet e cooperação internacional em matéria penal entre Brasil e Estados Unidos**. Rev. Bras. Polít. Públicas, Brasília, v. 8, nº 1, 2018 p.276-288, p. 284.

[92] GUIDI, Guilherme Berti de Campos; REZEK, Francisco. **Crimes na internet e cooperação internacional em matéria penal entre Brasil e Estados Unidos**. Rev. Bras. Polít. Públicas, Brasília, v. 8, nº 1, 2018 p.276-288, p. 285

[93] BRASIL. **Decreto N° 3.810**, de 2 de maio de 2001, Acordo de Assistência Judiciária em Matéria Penal entre Brasil e Estados Unidos. Disponível em http://www.planalto.gov.br/ccivil_03/decreto/2001/D3810.htm Acesso em: 28/05/2021

> execução especificado na solicitação deverá, contudo, ser seguido, exceto no que tange às proibições previstas nas leis do Estado Requerido.[94]

As solicitações entre ambos os países seguem diversos trâmites e especificidades, devendo conter informações claras sobre a autoridade que conduz a investigação relacionada com a solicitação, a matéria e natureza da investigação, do delito específico, da prova e da finalidade da prova, informações ou assistência pedidas (art. IV, item 2 do MLAT). Ainda é possível haver recusa da assistência quando delito for militar, mas não constituir crime comum, quando prejudicar a segurança ou interesses do Estado Requerido e quando não for feito em conformidade com o Acordo (Art. III item 1 do MLAT). Contudo, resta ainda estabelecido que, antes de negar a solicitação, as autoridades centrais dos países devem se comunicar para avaliar outras condições para prestação da assistência[95].

Isto posto, enfatiza-se que, segundo dados do Ministério da Justiça e Segurança Pública, em matéria penal, em 2020, a porcentagem mais alta de pedidos novos ativos representa 13,2% correspondente à cooperação jurídica internacional em matéria penal com os Estados Unidos[96]. Dessa forma, observa-se a importância da relação entre Brasil e Estados-Unidos, visto que a porcentagem frisa a necessidade da cooperação internacional.

3.2. A INEFICIÊNCIA DO MLAT E A AÇÃO DECLARATÓRIA DE CONSTITUCIONALIDADE N° 51 (ADC 51)

Dado o exposto sobre o MLAT entre o Brasil e os Estados Unidos, percebeu-se uma série de desafios devido às novas transformações digitais. Nesse contexto, foi ajuizada, pela Federação das Associações das Empresas de Tecnologia da Informação (ASSESPRO NACIONAL), a Ação Declaratória de Constitucionalidade n° 51, de 2017, visando discutir a constitucionalidade do Acordo de Assistência Legal Mútua (MLAT) entre Brasil e Estados-

---

[94] BRASIL. **Decreto N° 3.810**, de 2 de maio de 2001, Acordo de Assistência Judiciária em Matéria Penal entre Brasil e Estados Unidos. Disponível em http://www.planalto.gov.br/ccivil_03/decreto/2001/D3810.htm Acesso em: 28/05/2021

[95] BRASIL. **Decreto N° 3.810**, de 2 de maio de 2001, Acordo de Assistência Judiciária em Matéria Penal entre Brasil e Estados Unidos. Disponível em http://www.planalto.gov.br/ccivil_03/decreto/2001/D3810.htm Acesso em: 28/05/2021

[96] BRASIL. Ministério da Justiça e Segurança Pública. **Indicadores DRCI/SENAJUS.** Cooperação Jurídica Internacional. 2020. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-protecao/cooperacao-internacional/estatisticas/indicadores/indicadores-drci-2020-cooperacao-juridica-internacional.pdf Acesso em: 23/08/2021

Unidos, em relação ao compartilhamento de dados controlados por provedores de acesso à *internet* no exterior.

Para melhor compreensão acerca da ineficiência do meio, devem-se destacar os dados trazidos pelo Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional do Ministério da Justiça e Segurança Pública (DRCI/MJ) sobre o MLAT entre os dois países no tangente à quebra de sigilo telemático e obtenção dos dados telemáticos nos Estados-Unidos. Nesse sentido, em 2017, os Estados Unidos se encontravam em terceiro lugar como país mais demandado pelo Brasil em cooperação jurídica internacional, com cerca de 12% dos pedidos totais. Ainda, conforme último relatório do DRCI/MJ, essa porcentagem em abril de 2021 se encontra em 19,37%[97].

Segundo o referido departamento, o presente MLAT é o acordo bilateral mais relevante em matéria penal no Brasil, visto a alta utilização deste. Dentre os pedidos encaminhados, o DRCI ressalta que 97% destes são baseados no MLAT estabelecido entre os dois países, sendo aproximadamente 7,5% dentre estes para a quebra de sigilo e obtenção de dados telemático. Contudo, dentre os 108 pedidos de cooperação, relacionados aos dados telemáticos, em andamento no ano de 2017, apenas 28 se encontravam efetivamente em andamento nos Estados-Unidos, sendo 8 do ano de 2014, 8 do ano de 2015, 5 do ano de 2016 e 7 do ano de 2017. Portanto, percebe-se a lentidão do processo de cooperação, tendo em vista que os pedidos de 2014 que ainda se encontravam não concluídos em 2017[98].

Ainda, conforme o trazido pelo DRCI/MJ, 80 dos pedidos estavam encerrados, seja por uma resposta positiva, seja pela demora em responder. Dentre estes, 18 foram solicitações atendidas, 62 sem resultados, 49 com respostas negativas e 13 desistências pela demora, ressaltando um índice de 22,5% de aproveitamento relativos à obtenção de dados telemáticos e quebra de sigilo telemático. Nesse sentido, o DRCI/MJ ressalta algumas causas, jurídicas e procedimentais, que demonstram a lentidão do processo de cooperação.[99]

Em relação às causas jurídicas, tem-se: insuficiência de nexo causal, relacionada à demonstração do *"probable cause"*, sendo estes indícios suficientes de autoria e materialidade,

---

[97] Petição de apresentação de manifestação nº 10.426/2018, juntado aos autos da ADC nº 51 do STF. Disponível em: https://www.dropbox.com/s/jhzoho0ddufigv0/Of%C3%ADcio%20DRCI.pdf?dl=0 Acesso em: 04/06/21 p.17

[98] Petição de apresentação de manifestação nº 10.426/2018, juntado aos autos da ADC nº 51 do STF. Disponível em: https://www.dropbox.com/s/jhzoho0ddufigv0/Of%C3%ADcio%20DRCI.pdf?dl=0 Acesso em: 04/06/21, p. 19-20

[99] *Ibidem*, p. 22

previstos na lei americana como requisitos para autorização da quebra do sigilo telemático; solicitações envolvendo crimes contra a honra ou de preconceito, não amparados pela legislação americana pela falta do requisito da dupla incriminação; vedação da interceptação telemática em tempo real, dado que é uma prática vedada nas leis americanas, quando o pedido é exclusivamente feito por autoridade estrangeira.[100]

Em relação às causas procedimentais, tem-se: a desistência do pedido, visto que este perde sua utilidade pela demora à ser respondido pelas autoridades americanas; a volatilidade dos dados telemáticos, que ensejam sua perda por excesso de prazo de retenção obrigatória das empresas provedoras de serviço de *internet* ou por terem sido apagados; a não localização da conta ou do provedor; a criptografia ponta a ponta que não permite que haja uma quebra de sigilo visto que os dados não são transmitidos à outros que não o remetente ou o destinatário, impossibilitando a coleta destes dados; por fim, a recusa visto que os dados foram fornecidos pela via direta, no caso de serem feitas duas solicitações, pelo acordo e diretamente.[101]

Além disso, conforme o DRCI/MJ a média de tempo para serem atendidas as diligências envolvendo a quebra do sigilo telemático giram em torno de 13 meses por meio do mecanismo do MLAT. Nesse âmbito, salienta-se que os dados telemáticos se tratam de provas altamente voláteis e necessárias às investigações cibernéticas, por essa razão a demora em relação ao atendimento dos pedidos representa um obstáculo ao processo que precisa ser resolvido.

No Ofício 28.725/2017, o DRCI/MJ ao prestar as informações abordadas acima, conclui que a legislação interna dos Estados-Unidos torna o procedimento lento e moroso, logo, evidenciando a ineficácia do meio para a requisição de dados telemáticos. Sendo assim, foi ressaltado que houve a inciativa brasileira de propor um Protocolo Adicional ao MLAT estabelecido entre os países, visando sanar as dificuldades abordadas, entretanto a reposta dada ao pedido brasileiro foi negativa no início do ano de 2018, conforme aponta o DRCI/MJ.[102] Em vista disso, o Dr. Marconi Costa Melo, do Departamento de Recuperação de Ativos, evidenciou em audiência pública, residida no dia 10 de fevereiro de 2020 para discussão da ADC 51, que

---

[100] Petição de apresentação de manifestação nº 10.426/2018, juntado aos autos da ADC nº 51 do STF. Disponível em: https://www.dropbox.com/s/jhzoho0ddufigv0/Of%C3%ADcio%20DRCI.pdf?dl=0 Acesso em: 04/06/21. p. 22-27

[101] Petição de apresentação de manifestação nº 10.426/2018, juntado aos autos da ADC nº 51 do STF. Disponível em: https://www.dropbox.com/s/jhzoho0ddufigv0/Of%C3%ADcio%20DRCI.pdf?dl=0 Acesso em: 04/06/21, p. 26-28

[102] Petição de apresentação de manifestação nº 10.426/2018, juntado aos autos da ADC nº 51 do STF. Disponível em: https://www.dropbox.com/s/jhzoho0ddufigv0/Of%C3%ADcio%20DRCI.pdf?dl=0 Acesso em: 04/06/21, p. 30-31

o mecanismo do MLAT não se trata de um mecanismo inconstitucional, contudo, apresenta resultados insatisfatórios[103].

Diante desse cenário, foram abordadas questões relacionadas à jurisdição, ressaltando que a Lei do Marco Civil traz um mecanismo de obtenção de dados, por meio do art. 11, em que se aborda a aplicação da legislação brasileira quando as operações de coleta, armazenamento, guarda e tratamento de dados se dê nos seguintes casos: em território brasileiro; com ao menos um dos terminais no Brasil; oferta de serviço ao público brasileiro; e, por fim, quando integrante do mesmo grupo econômico tenha estabelecimento no Brasil. Faz-se necessário ainda ressaltar, que o art. 3°, parágrafo único da mesma lei, por sua vez, estabelece que "Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte", ressaltando a aplicação dos tratados e convenções, e portanto sua compatibilidade com estes.[104]

A questão envolvendo a competência para requisição dos dados e a recusa pelos Estados-Unidos em entregar os referidos dados, uma vez contrapostas com as legislações americanas, se tornou um ponto central na discussão em audiência pública. Dessa forma, surgiu a indagação em relação ao *Cloud Act,* abordado como solução para alguns e perpetuação do mesmo problema para outros. Nesse âmbito, o relator, Excelentíssimo Ministro Gilmar Mendes, questionou aos requerentes (ASSESPRO NACIONAL), acerca do referido instrumento, ocasião em que o representante da referida associação e o representante do Facebook manifestaram-se positivamente sobre a possibilidade de um acordo por este meio com o Brasil.[105]

O Excelentíssimo Ministro Gilmar Mendes ressaltou os pontos trazidos em audiência abordando a nova possibilidade de cooperação por meio do *Cloud Act*, finalizando a sessão pública em seguida. No contexto da Ação Declaratória de Constitucionalidade n° 51, o

---

[103] SUPREMO TRIBUNAL FEDERAL. **Ata da Audiência Pública ADC n° 51**. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADC51Transcricoes.pdf Acesso em: 16/06/2021

[104] BRASIL. **Lei N° 12.965**, de 23 de abril de 2014. Marco Civil da Internet, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acesso em: 16/06/2021

[105] SUPREMO TRIBUNAL FEDERAL. **Ata da Audiência Pública ADC n° 51**. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADC51Transcricoes.pdf Acesso em: 16/06/2021

surgimento do tema gera questionamentos acerca da aplicabilidade do *Cloud Act*, assim como do seu funcionamento e das possíveis vantagens de integrá-lo.

3.3. O ADVENTO DO *CLOUD ACT:* POSSÍVEL SOLUÇÃO

O *Clarifying Lawful Overseas Use of Data Act*, apelidado de *Cloud Act*, trata-se da lei, aprovada em 2018, pelos Estados-Unidos, para fazer face à necessidade da rápida obtenção de dados para investigações. A lei busca dialogar com duas questões principais, a requisição de dados pelos Estados-Unidos em relação às empresas americanas no exterior e a requisição de dados por outros países em relação às empresas nos Estados-Unidos.

Dessa maneira, como alternativa para cooperação internacional em requisição de dados, o *Cloud Act* traz os acordos executivos, possibilitando aos países obterem os dados diretamente dos provedores americanos. Deve-se ressaltar que o primeiro acordo executivo, sob a égide do *Cloud Act*, se deu em outubro de 2019 entre os Estados-Unidos e o Reino Unido. Destaca-se que para que seja possível o acordo executivo entre um país e os Estados-Unidos, tem-se alguns requisitos a serem seguidos.

Em primeiro lugar, o país que busca adentrar um acordo executivo deve observar em sua lei doméstica, a proteção da privacidade e das liberdades civis, adotando leis pertinentes com a convenção. Da mesma forma, é abordado o respeito ao princípio da não discriminação e aos direitos humanos, incluindo: proteção às interferências arbitrárias na privacidade; direito ao julgamento justo; liberdade de expressão, associação e reunião pacífica; proibição de prisões e detenções arbitrárias; e, criminalização da tortura, tratamento cruel, desumano, degradante ou punitivo.[106]

Ainda acerca da proteção da privacidade e liberdades civis, é demandado que o país requerente tenha procedimentos e mandatos claros para autorização da obtenção de dados pelo acordo executivo, incluindo os procedimentos de coleta, retenção, uso e compartilhamento e supervisionamento dessas atividades. Igualmente, requer-se mecanismos de transparência para coleta e uso de dados e demonstração de compromisso para promover e proteger o fluxo livre global de informações e a natureza aberta da *internet.*[107]

---

[106] ESTADOS UNIDOS. 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: 18/06/2021

[107] ESTADOS UNIDOS. 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: 18/06/2021

Em segundo lugar, deve ser observado que o país acordante não poderá, intencionalmente, visar uma pessoa localizada ou de nacionalidade americana, sendo estas cidadãs, nacionais ou nacionalizados, associações sem personalidade jurídica (*unincorporated associations)* com membros americanos ou corporações americanas. Da mesma forma, não poderá visar indivíduos para obter informações sobre um cidadão americano ou os entes abordados. Não poderá o governo da parte acordante requerer informações acerca do governo americano.[108]

Em relação aos requerimentos, estes devem ser elaborados motivadamente, apresentando o nexo causal e especificando as informações necessárias para o cumprimento, que se dará conforme a lei nacional do requerente. Estarão, ainda, sujeitos à revisão ou análise de um magistrado ou outra autoridade independente. Ademais, a referida lei prevê a hipótese de requerimento da interceptação telefônica, tendo como requisitos o tempo limitado e a subsidiariedade, logo, se não houver outro meio para obtenção da prova. Contudo, resta estabelecido que o referido acordo executivo tem em vista a prevenção, detecção e investigação de crimes ditos "sérios", incluindo neste conceito o terrorismo, entretanto sem definir o que seriam crimes sérios[109].

Dessa forma, o novo instrumento abordado remove as proibições da antiga Lei *Electronic Communications Privacy Act*, permitindo que os países estrangeiros emitam ordens, seguindo suas leis nacionais, garantindo que a lei da outra parte não será uma barreira para o cumprimento quando no requerimento de dados de um provedor americano e que estes possam responder diretamente, sem penalidades civis ou criminais.[110] Nesse sentido, o acordo executivo estabelecido entre os Estados-Unidos e o Reino Unido, art. 3°, parágrafo primeiro prevê que cada parte se utilizará de suas leis domesticas para preservação, autenticação, divulgação e produção de dados eletrônicos permitindo aos provedores o atendimento às ordens emitidas sob o acordo executivo.[111]

---

[108] ESTADOS UNIDOS. 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: 18/06/2021

[109] ESTADOS UNIDOS. 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: 18/06/2021

[110] MULLIGAN, Stephen P. **Cross-Border Data Sharing Under the CLOUD Act, report**, 23 de Abril, 2018. Washington D.C. (https://digital.library.unt.edu/ark:/67531/metadc1156725/), University of North Texas Libraries, UNT Digital Library, https://digital.library.unt.edu; crediting UNT Libraries Government Documents Department. p. 19

[111] AGREEMENT between the government of The United State of America and the government of The United Kingdom of Great Britain and Northern Ireland on access to electronic data for the purpose of countering serious crime. 2019. Disponível em:

Conforme explanado ao longo do presente estudo, permite-se concluir que o Brasil possui os requisitos para cooperação com os Estados-Unidos, por meio do acordo executivo do *Cloud Act.* Com o advento da Lei Geral de Proteção de Dados Pessoais se demonstram cumpridos os requisitos acerca da proteção da privacidade e de dados requerida. A possível futura adesão à Convenção de Budapeste, em processo de análise atual pelo Brasil preenche o outro requisito demandado pela lei americana. Assim sendo, possivelmente, o *Cloud Act* pode se tornar uma solução à ineficácia do MLAT observado que dentre os desafios evidenciados, o acordo executivo do *Cloud Act* propicia a solução acerca da aplicabilidade da lei e dá celeridade ao processo de coleta de dados, representando um avanço na esfera da investigação de cibercrimes.

CONSIDERAÇÕES FINAIS

Dado o desenvolvimento tecnológico crescente que permeia e se relaciona com o mundo do Direito, os cibercrimes vêm ocupando a esfera dos delitos, surgindo novos tipos penais, ou ainda, tipos penais digitalizados. Destacado o caráter transnacional, de natureza volátil e específica das provas nos delitos digitais, as perícias especializadas se tornam necessárias, originando o conceito de "*Cloud Computing"*, ensejando uma perícia em nuvem.

Ainda, a relevância da cooperação internacional se destaca na medida em que se torna essencial para a coleta de evidências acerca do crime virtual cometido, gerando um trânsito de dados entre os países. Na esfera internacional, observa-se o papel da Convenção de Budapeste, também denominada Convenção de Cibercrimes, que buscou delimitar alguns aspectos da cooperação internacional para a correta coleta de dados na investigação dos referidos crimes. Na esfera brasileira, destaca-se que o trânsito de dados esbarra em duas leis criadas para regular o uso da *internet* e o uso de dados, a Lei do Marco Civil da Internet e a Lei Geral de Proteção de Dados, respectivamente.

Dessa forma, a presente monografia discutiu os aspectos, materiais e processuais, que delimitam a cooperação internacional na esfera da investigação de cibercrimes. Além disso,

---

https://www.justice.gov/ag/page/file/1207496/download#Agreement%20between%20the%20Government%20of%20the%20United%20States%20of%20America%20and%20the%20Government%20of%20the%20United%20Kingdom%20of%20Great%20Britain%20and%20Northern%20Ireland%20on%20Access%20to%20Electronic%20Data%20for%20the%20Purpose%20of%20Countering%20Serious%20Crimes Acesso em:18/06/2021

observou o posicionamento do Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional, que lida diretamente com a requisição de dados para investigação cibernética, para constatar a ineficiência do presente instrumento de Acordo de Assistência Judiciária em Matéria Penal entre o Brasil e os Estados-Unidos. A Ação Declaratória de Constitucionalidade n° 51 permitiu que fossem permeados diversos posicionamentos acerca da utilização de outro instrumento de cooperação internacional, restando a questão inconclusa.

Nesse sentido, surge a possibilidade da aplicação do instrumento americano recente trazido pela lei, aprovada em 2018, *Clarifying Lawful Overseas Use of Data Act (Cloud Act).* A previsão de acordos executivos ressaltada na lei traz um novo aspecto da cooperação internacional, sendo possível a aplicação da lei doméstica na requisição de dados. Fato esse que tornou o MLAT entre os dois países lento e prejudicou a adequada investigação e obtenção de dados. Em vista disso, o *Cloud Act* se torna uma possível solução a ser trazida para o âmbito brasileiro na cooperação internacional com os Estados Unidos, possuidor de um grande *data center*.

Necessário destacar que, segundo indicadores providos pelo Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional, em 2020, relativos à matéria penal, a porcentagem de pedidos novos passivos feitos pelos Estados Unidos ao Brasil representam uma porcentagem de apenas 1,8%[112]. Contudo, os pedidos novos ativos direcionados aos Estados Unidos, em 2020, representavam uma porcentagem de 13,2%[113]. Portanto, há uma discrepância dos pedidos ativos e passivos no Brasil, que permite constatar a dependência em relação ao trânsito de dados, principalmente com os Estados Unidos. Nesse âmbito, o debate acerca da troca justa e igualitária entre os países deve ser abordado e ampliado para pesquisas futuras.

Sendo assim, a discussão acerca dos instrumentos para requisição de dados entre países se tona essencial para desenvolver a temática da cooperação internacional observando as peculiaridades das provas nos crimes virtuais. Ainda, por ser uma temática recente, os atores

---

[112] BRASIL. Ministério da Justiça e Segurança Pública. **Indicadores DRCI/SENAJUS.** Cooperação Jurídica Internacional. 2020. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-protecao/cooperacao-internacional/estatisticas/indicadores/indicadores-drci-2020-cooperacao-juridica-internacional.pdf Acesso em: 23/08/2021

[113]BRASIL. Ministério da Justiça e Segurança Pública. **Indicadores DRCI/SENAJUS.** Cooperação Jurídica Internacional. 2020. Disponível em: https://www.gov.br/mj/pt-br/assuntos/sua-protecao/cooperacao-internacional/estatisticas/indicadores/indicadores-drci-2020-cooperacao-juridica-internacional.pdf Acesso em: 23/08/2021

estão buscando adaptar suas leis domésticas ao cenário atual, criando uma insegurança jurídica internacional acerca da requisição de dados, que ainda não se consolidou de forma homogênea.

Logo, os cibercrimes devem ser analisados e discutidos, assim como as formas de cooperação para coleta de dados pessoais durante o procedimento investigatório. A reflexão acerca dos instrumentos de cooperação se observa essencial para uma aplicação justa e correta dos acordos entre os países permeados pelos delitos virtuais. Nesse sentido, abre-se um novo debate em relação à perspectiva da cooperação internacional, envolvendo a colaboração entre países de maneira efetiva e igualitária, observando vantagens para ambas as partes do acordo e respeitando as legislações domésticas, além do direito à privacidade e o correto manuseio dos dados.

REFERÊNCIAS

AGREEMENT between the government of The United State of America and the government of The United Kingdom of Great Britain and Northern Ireland on access to electronic data for the purpose of countering serious crime. 2019. Disponível em: https://www.justice.gov/ag/page/file/1207496/download#Agreement%20between%20the%20Government%20of%20the%20United%20States%20of%20America%20and%20the%20Government%20of%20the%20United%20Kingdom%20of%20Great%20Britain%20and%20Northern%20Ireland%20on%20Access%20to%20Electronic%20Data%20for%20the%20Purpose%20of%20Countering%20Serious%20Crimes Acesso em:18/06/2021

ASSOCIAÇÃO NACIONAL DOS PROCURADORES DA REPÚBLICA, **Proteção de dados pessoais e investigação criminal**, 3ª Câmara de Coordenação e Revisão. Ministério Público Federal e Organizadores: Vladimir Barros Aras, Andrey Borges de Mendonça, Walter Aranha Capanema, Carlos Bruno Ferreira da Silva e Marcos Antônio da Silva Costa. Brasília: ANPR, 2020

AVENA, Noberto, **Processo Penal.** Rio de Janeiro: Método, 2020. 12, rev., atual., ampl.

BOMFATI, Claúdio Adriano; KOLBE JUNIOR, Armando. Crimes cibernéticos. Ed. 1. Curitiba: Intersaberes, 2020.

Brasil é convidado a aderir à Convenção do Conselho da Europa contra a Criminalidade Cibernética. Secretaria-Geral. Disponível em: <https://www.gov.br/secretariageral/pt-br/noticias/2020/julho/brasil-e-convidado-a-aderir-a-convencao-do-conselho-da-europa-contra-a-criminalidade-cibernetica>. Acesso em: 14/05/21.

BRASIL, Ministério Público Federal, **Crimes Cibernéticos:** manual prático de investigação, 2006.

BRASIL. **Decreto N° 3.810,** de 2 de maio de 2001, Acordo de Assistência Judiciária em Matéria Penal entre Brasil e Estados Unidos. Disponível em http://www.planalto.gov.br/ccivil_03/decreto/2001/D3810.htm Acesso em: 21/05/2021

BRASIL. **Decreto N° 8.771**, de 11 de maio de 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/D8771.htm Acesso em: 07/05/2021

BRASIL. **Decreto-Lei Nº 3.689**, 3 de outubro de 1941. Código de Processo Penal, 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm. Acesso em: 16/04/2021

Brasil é convidado a aderir à Convenção do Conselho da Europa contra a Criminalidade Cibernética. **Secretaria-Geral**. Presidência da República. Notícias, julho 2020, 24/07/2020. Disponível em: https://www.gov.br/secretariageral/pt-br/noticias/2020/julho/brasil-e-convidado-a-aderir-a-convencao-do-conselho-da-europa-contra-a-criminalidade-cibernetica. Acesso em: 14/05/21.

BRASIL. **Lei N° 11.419**, de 19 de dezembro de 2006. Lei do Processo Eletrônico, 2006. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11419.htm. Acesso em: 16/04/2021

BRASIL. **Lei N° 12.682**, de 9 de julho de 2012. Elaboração e arquivamento de documentos em meios eletromagnéticos, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12682.htm. Acesso em: 16/04/2021

BRASIL. **Lei N° 12.965**, de 23 de abril de 2014. Marco Civil da Internet, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm Acesso em: 30/04/2021

BRASIL. **Lei N° 13.105**, de 16 de março de 2015. Código de Processo Civil, 2015. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 16/04/2021

BRASIL. **Lei N° 13.709**, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm Acesso em: 07/05/2021

BRASIL. **Lei Nº 10.406**, 10 de janeiro de 2002. Código Civil, 2002. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 16/04/2021

BRASIL. Ministério da Justiça e Segurança Pública. **Indicadores DRCI/SENAJUS.** Cooperação Jurídica Internacional. 2020

BRASIL. Ministério Público Federal**. Roteiro de atuação**: crimes cibernéticos. 2 ed. rev. - Brasília: MPF/2ªCCR, 2013.

BRASIL. Tribunal Regional Federal da 3ª Região. Escola de Magistrados **Investigação e prova nos crimes cibernéticos**. São Paulo: EMAG, 2017.

CAIADO, Felipe B., CAIADO, Marcelo, **Combate à pornografia infantojuvenil com aperfeiçoamentos na identificação de suspeitos e na detecção de arquivos de interesse,** Crimes cibernéticos: coletânea de artigos: Brasília: MPF, 2018.

CANEIRO, Márcio Rodrigo de Freitas, **Perícia de informática nos crimes cibernéticos**, Tribunal Regional Federal da 3ª Região. Escola de Magistrados Investigação e prova nos crimes cibernéticos. São Paulo: EMAG, 2017.

COUNCIL OF EUROPE. **Convenção sobre o Cibercrime**. Budapest, 23.XI.2001. Acesso em: https://rm.coe.int/16802fa428 . Acesso em: 14/05/21

COUNCIL OF EUROPE. **Relatório Explicativo da Convenção de Budapeste**, 23, XI,2001. Disponível em: https://rm.coe.int/16802fa429 Acesso em 14/05/21

DE OLIVEIRA DOS SANTOS, Thiago; FERREIRA MONTENEGRO DUARTE, Bruno. A Responsabilidade Civil Dos Provedores De Aplicação De Internet No Tratamento De Dados À Luz Da Lei. No 12.965/2014 Denominada O Marco Civil Da Internet. **Revista Eletrônica de Direito da Faculdade Estácio do Pará**, [S.l.], v. 5, n. 7, p. 79 - 100, jun. 2018. ISSN 2359-3229, p.84 Disponível em: <http://revistasfap.com/ojs3/index.php/direito/article/view/193>. Acesso em: 30 abr. 2021.

DELGADO, Vladimir Chaves. **Cooperação internacional em matéria penal na convenção sobre o cibercrime**. 2007, 315 p. Dissertação (Mestrado em Direito das Relações Internacionais) – Centro Universitário de Brasília, Brasília, 2012

DIDONÉ, Dener; José Guerra Barreto de Queiroz, Ruy. **Computação em nuvem: desafios e oportunidades para a forense computacional.** 2011. 112 f. Dissertação (Mestrado). Programa de Pós-Graduação em Ciência da Computação, Universidade Federal de Pernambuco, Recife, 2011

DOMINGOS, Fernanda Teixeira Souza; RÖDER, Priscila Costa Schereiner, **Obtenção de provas digitais e jurisdição na internet**, Ministério Público Federal. Câmara de Coordenação e Revisão, 2. Crimes cibernéticos, 2ª Câmara de Coordenação e Revisão, Criminal, Brasília: MPF, 2018.

ESTADOS UNIDOS. 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: 18/06/2021

GUIDI, Guilherme Berti de Campos; REZEK, Francisco. **Crimes na internet e cooperação internacional em matéria penal entre Brasil e Estados Unidos**. Rev. Bras. Polít. Públicas, Brasília, v. 8, nº 1, 2018 p.276-288

JESUS, Damásio de; MILAGRE, José Antonio. Manual de crimes informáticos. São Paulo: Saraiva, 2016.

LEXISNEXIS RISK SOLUTIONS CYBERCRIME REPORT. **The changing face of cybercrime.** Digital Identity Network, Janeiro-Junho 2020. Relatório.

LIMA, Caio César Carvalho, **Aspectos legais da Perícia Forense Computacional em um cenário de Cloud Computing,** In: PROCEEDING OF THE FIFTH INTERNATIONAL CONFERENCE ON FORENSIC COMPUTER SCIENCE. Brasília: ICoFCS 2010 ABEAT (ed.), 2010.

LOPES JR, Aury. **Direito processual penal**. São Paulo: Saraiva, 2020. 17, 2020

MARTINS, Dheneb. **Investigação Cibernética**. Ed. 1. Curitiba: Contentus, 2020.

MULLIGAN, Stephen P. **Cross-Border Data Sharing Under the CLOUD Act, report**, 23 de Abril, 2018. Washington D.C. (https://digital.library.unt.edu/ark:/67531/metadc1156725/), University of North Texas Libraries, UNT Digital Library, https://digital.library.unt.edu; crediting UNT Libraries Government Documents Department.

NUCCI, Guilherme de Souza. **Manual de Processo Penal.** Rio de Janeiro: Forense, 2021. 2, rev., atual., ampl.

PECK, Patricia. **Direito digital.** São Paulo: Saraiva Educação, 6ª edição, 2016.

Petição de apresentação de manifestação nº 10.426/2018, juntado aos autos da ADC nº 51 do STF. Disponível em: https://www.dropbox.com/s/jhzoho0ddufigv0/Of%C3%ADcio%20DRCI.pdf?dl=0 Acesso em: 04/06/21

ROCHA, Lilian Rose Lemos (coord.) et al. **Caderno de pós-graduação em direito**: Crimes digitais. Brasília: UniCEUB: ICPD, 2020.

ROMANOSKI, Vanderlei et al. **Forense computacional e a garantia das evidências no uso da computação em nuvem numa organização**. Curso de Especialização em Gestão da Segurança da Informação-Unisul Virtual, 2019

SUPREMO TRIBUNAL FEDERAL. **Ata da Audiência Pública ADC n° 51**. Disponível em: http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADC51Transcricoes.pdf Acesso em: 16/06/2021

TEIXEIRA, Tarcisio, **Direito digital e processo eletrônico**,5. ed., São Paulo: Saraiva Educação, 2020.

Turmas remarcam sessões previstas para esta terça-feira (10), **Superior Tribunal de Justiça**, 09/11/2020. Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/09112020-Turmas-remarcam-sessoes-previstas-para-esta-terca-feira--10-.aspx Acesso em: 25/11/2020