OS CRIMES CIBERNÉTICOS NO ORDENAMENTO JURÍDICO BRASILEIRO: INVESTIGAÇÃO CRIMINAL E DESAFIOS

CYBERCRIMES IN THE BRAZILIAN LEGAL SYSTEM: CRIMINAL INVESTIGATION AND CHALLENGES

Liv Ferreira Augusto Severo Queiroz
Bacharel em direito pela Universidade Federal do Rio de Janeiro (UFRJ). Promotora de Justiça titular da 2ª Promotoria de Justiça de Apodi/RN. Coordenadora de Investigações Especiais do Grupo de Atuação Especial de Combate ao Crime Organizado do MPRN (GAECO). Coordenadora do Centro de Apoio às Promotorias do Patrimônio Público do MPRN (CAOP-PP).
E-mail: livsevero@gmail.com

Recebido em: 22/6/2024 | Aprovado em: 29/8/2024

Resumo: O presente artigo objetiva analisar os tipos de crimes cibernéticos, modos de investigação criminal, especificidades e desafios. Discorre sobre pontos relevantes da Lei do Marco Civil da Internet (Lei 12.965/2014) e da Convenção de Budapeste, fortes instrumentos de investigação criminal no meio virtual. Ressalta a importância do pedido de preservação dos dados digitais aos provedores de Internet em razão da volatilidade da prova digital. Destaca a relevância de qualificar as autoridades para investigação cibernética por ser esta a investigação criminal do futuro, alcançando também os crimes comuns não praticados no âmbito virtual, mas cujas as provas encontram-se armazenadas virtualmente.

Palavras-chave: Crimes cibernéticos; Prova Digital; Preservação de Dados; Lei do Marco Civil da Internet; Convenção de Budapeste.

Abstract: *The article deals with cybercrimes, methods of criminal investigation, specificities and challenges. Discusses relevant points of the Internet Civil Framework Law (Law 12,965/2014) and the Budapest Convention, which came into force in the legal system in March 2023. Highlights the importance of requesting the*

preservation of digital data from Internet providers due to the volatility of digital proof. It highlights the relevance of qualifying authorities for cyber investigation as this is the criminal investigation of the future, also covering common crimes not committed in the virtual sphere, but for which the evidence is stored virtually.

Keywords: *Cybercrimes; Digital Proof; Data Preservation; Internet Civil Rights Framework Law; Budapest Convention.*

INTRODUÇÃO

A Internet tem sido utilizada para as mais diversas finalidades, como a realização de pesquisas, compras, operações financeiras ou comerciais, manutenção de redes sociais, busca de amizades e relacionamentos amorosos, além de outros propósitos legais. Por outro lado, a rede mundial de computadores também tem sido campo fértil para a prática dos mais diversos crimes cibernéticos, próprios e/ou impróprios.

Os tipos de crimes cibernéticos, conceitos, características e previsão na legislação brasileira são temas relevantes para que se obtenha o conhecimento prévio de qual conduta criminosa será a investigada. Por outro lado, não obstante a distinção de conceitos, a coleta de provas digitais é realizada com as mesmas cautelas em todos os tipos de crimes que tenham como objeto de investigação os dados digitais/informáticos.

A compatibilidade dos tipos penais cibernéticos existentes atualmente no ordenamento jurídico brasileiro com as legislações pátrias penais e processuais penais, assim como com a Convenção de Budapeste, é outro ponto de relevância a ser tratado na análise dos crimes cometidos no âmbito virtual, mormente quando se traz à lume a cooperação internacional.

Assunto de extrema importância refere-se à coleta das provas digitais e a necessidade de que seja realizada adequadamente, medida esta imprescindível ao enfrentamento do crime organizado, das práticas de pedofilia, e dos demais crimes praticados na rede mundial de computadores. Isto porque a coleta equivocada da prova ou a "não coleta" poderá acarretar a perda definitiva do lastro probatório pretendido, tendo em vista que a prova digital é volátil e, na maioria das vezes, irrepetível.

Questões relevantes da Lei do Marco Civil serão ressaltadas neste artigo, como por exemplo, a necessidade de preservação de dados digitais tão logo surjam informações suficientes para formular tal requerimento aos provedores de Internet, sob pena de perda da prova e a obrigatoriedade do fornecimento de dados cadastrais às autoridades brasileiras, independentemente de ordem judicial.

A promulgação da Convenção de Budapeste, e sua vigência no ordenamento jurídico a partir do ano de 2023, trouxe medidas eficazes e céleres à obtenção da prova digital com a finalidade de enfrentar e combater os agentes de cibercrimes, mediante cooperação internacional.

Por fim, os aspectos controvertidos da investigação criminal na seara cibernética também se desnudam, mormente os desafios diante do uso de mecanismos de anonimização de dados, e o compartilhamento de um mesmo IP por diversos usuários, seja em razão de um costume doméstico ou em decorrência da utilização do GNAT[1] pelos provedores de conexão como forma de compartilhar a diversos usuários um mesmo IPV4, mecanismos estes que dificultam, e por vezes, inviabilizam, o prosseguimento das investigações criminais.

1. A INVESTIGAÇÃO DE CRIMES CIBERNÉTICOS NO ORDENAMENTO JURÍDICO BRASILEIRO E SEUS DESAFIOS

Crimes cibernéticos são aqueles que no contexto da atividade criminal são cometidos ou facilitados pela rede mundial de computadores (Internet), assim como pelo abuso ou mau uso de sistemas e aplicativos diversos.

O escopo principal deste artigo é demonstrar de forma objetiva a necessidade de elaboração de uma legislação penal e processual específicas, a fim de tomar mais efetivo o combate ao crime cibernético.

A qualificação das autoridades para atuação em delitos dessa natureza é imprescindível em razão da volatilidade da prova digital que restará perdida de forma definitiva se não for preservada tempestivamente

1 A *Carrier Grade Network Address Translation* (CGNAT) e uma solução utilizada por provedores de serviços de Internet, que oferece conectividade e experiência de usuário ininterrupta para seus clientes. A técnica é utilizada por operadoras de telecomunicação em situação crítica, que não tem mais endereços IPv4 disponíveis. Um dos efeitos mais negativos do CGNAT é a dificuldade de identificar o autor de um determinado crime ou fraude.

e de modo adequado, sendo estes um dos maiores desafios na investigação criminal.

Em razão da popularização do acesso à Internet e da expansão de redes sociais, a prática de crimes cibernéticos no Brasil tem avolumado-se a cada ano, gerando, consequentemente, um aumento expressivo de vítimas de crimes dessa natureza.

Os crimes cibernéticos dividem-se em "crimes cibernéticos impróprios" e "crimes cibernéticos próprios". Os primeiros, podem ser praticados da forma tradicional ou por intermédio de computadores, ou seja, o computador apresenta-se apenas como meio para a prática do crime, como no caso dos delitos de ameaça, racismo, estelionato, crimes contra a honra, falsificação de documentos, dentre outros previstos no Código Penal e em legislações esparsas.

Os "crimes cibernéticos próprios" somente podem ser praticados com a utilização de computadores ou qualquer outro dispositivo eletrônico que possibilite o acesso à Internet. O meio informático é o instrumento utilizado para a pratica do crime e também, a depender do tipo penal cometido, e do bem jurídico tutelado. É a hipótese do art.154 - A (invadir dispositivo informático alheio), art.313-A (inserção de dados falsos em sistema de informações) alem de outros existentes na legislação penal vigente.

Há ainda uma terceira categoria, a dos "crimes cibernéticos mistos", nos quais o uso da Internet é condição indispensável para que a ação criminosa se efetive, mesmo que se vise atingir outro bem jurídico, diverso do sistema informático. É o exemplo do crime previsto no Estatuto da Criança e do Adolescente, no artigo 244-B, §1° que dispõe a respeito do crime de corrupção de menores em salas de bate papo da Internet e que apenas pode ser cometido através de dispositivos eletrônicos, no entanto, o bem jurídico tutelado, e diverso, qual seja, a proteção dos direitos fundamentais da criança e do adolescente.

O ordenamento jurídico brasileiro não possui uma norma penal unificada que concentre os tipos penais cibernéticos ao quais se encontram localizados em leis esparsas, como na Lei de Interceptação Telefônica (art.10 da Lei 9296/1996), Estatuto da Criança e do Adolescente (art.241-B

e art.244-D), Lei 9.609/1998 (art.12), Lei 9.504/97 (art.72), Código Penal (art.154-A), entre outras normas legais.

Importante consignar que a investigação de cibercrimes, próprios ou impróprios, ou ainda, mistos, a depender da classificação adotado pelo operador do direito, exige cada vez mais o acesso às provas digitais cuja coleta requer procedimentos específicos, e necessários, sobretudo, à preservação dos ditos dados e das provas de natureza digital.

Muitos são os crimes cibernéticos praticados habitualmente que sequer são investigados, não apenas pela falta de capacitação das autoridades que recebem a notícia do crime, como por vezes, pela ausência de ferramentas forenses necessárias à extração dos dados. E há hipótese em que a investigação tem seu início deflagrado, contudo, sem êxito na identificação da autoria, pelos mesmos motivos já explicitados.

Se por um lado a complexidade da investigação obsta a identificação da autoria por não ter aquele que investiga a qualificação adequada para atuar, por outro, ao criminoso não se faz necessário na maioria das vezes qualquer conhecimento técnico de informática, jurídico ou forense mas tão somente o dolo de agir e a criatividade para colocar em prática a empreitada criminosa.

A *engenharia social* é muito usada para o cometimento de crimes na seara virtual, trata-se da utilização de um conjunto de técnicas destinadas a ludibriar a vítima de forma que acredite nas informações prestadas pelo criminoso e se convença a fornecer, de forma voluntária, seus próprios dados pessoais possibilitando que, através destes, seja possível praticar o crime pretendido pelo meliante.

Isto é, geralmente os criminosos simulam fazer parte de instituições confiáveis, como bancos, sites de compras, órgãos públicos, para que a vítima acredite nos falsos dados apresentados. Trata-se, na realidade, da isca para que sejam obtidas informações muitas vezes sigilosas, como por exemplo, a senha de uma conta bancária, de um cartão de crédito ou até mesmo de um aplicativo de mensagens.

Verifica-se, portanto, que enquanto algumas ameaças cibernéticas utilizam vulnerabilidades de uma rede ou servidor, na *engenharia social* o criminoso concentra-se nas vulnerabilidades das próprias vítimas.

"Golpes" cibernéticos notórios como o "sequestro" da conta do *WhatsApp,* em que o criminoso passa a usá-la para pedir transferência de valores aos contatos da agenda da vítima, nada mais são do que o uso de *engenharia social*. É o próprio usuário da conta quem repassa a senha ao meliante permitindo que este proceda à instalação da conta de *WhatsApp* em seu telefone fazendo-se passar pela própria vítima para solicitar transferências em dinheiro de amigos e parentes.

Crimes cibernéticos mais complexos também são praticados, como por exemplo, a utilização de arquivos maliciosos que permitem ao criminoso o acesso remoto ao computador da vítima obtendo assim dados confidenciais. É a hipótese do arquivo malicioso denominado *trojan horse* (Cavalo de Tróia) cuja estratégia consiste em encaminhar um arquivo que ao ser executado compromete o computador da vítima de modo que o invasor possa tê-lo em seu domínio, permitindo assim que o computador do criminoso acesse a outra máquina à distância e obtenha dados confidenciais daquela.

Outra forma de ataque cibernético que criptografa os dados de um usuário ou empresa restringindo o acesso a informações essenciais é o *ransomware*. Esta conduta, crime de sequestro de dados ou *ransomware,* não é tipificada especificamente no ordenamento penal brasileiro[2], e se perfaz mediante obtenção de acesso ao sistema informático com uso de ardil que induz o proprietário ou titular da máquina ao engano, para, ato contínuo, inserir um código fonte com o intuito de bloquear o acesso por usuário que não possua a senha descodificadora. Após lograr êxito na empreitada criminosa, o agente comunica-se com a vítima exigindo desta o montante de dinheiro, geralmente em bitcoin ou outra criptomoeda, para que haja a liberação e recuperação dos dados criptografados.

Como forma de dificultar a investigação do crime, mormente a identificação da autoria, o pagamento desse "resgate", via de regra, costuma ser feito com o uso de criptomoedas, já que, além do valor econômico elevado, há ainda, a notória dificuldade de rastreabilidade do destinatário da quantia econômica em operações dessa natureza.

2 No Brasil, via de regra, tipifica-se o ataque de *ransomware* como um crime de extorsão, previsto no art.158 do Código penal, com penas que variam de 4 a 10 anos de prisão.

Estas são apenas algumas das modalidades utilizadas para a prática do crime cibernético, havendo, contudo, um amplo rol de mecanismos de ataques dessa natureza permitindo que as vítimas sofram os mais variados tipos de danos, seja na esfera financeira, como nos casos de fraude bancária, estelionato virtual, entre outros, ou no abalo de sua própria honra, nas hipóteses de *Cyberbullying* quando são realizadas ofensas de naturezas diversas que rapidamente são disseminadas na rede mundial de computadores. Ressalte-se, também, os casos de *Cyberstalking* no qual se persegue alguém mediante reiteração de atos que têm como finalidade principal causar o pânico e a insegurança usando como ferramenta a plataforma digital.

Para que o crime cibernético tenha a sua autoria evidenciada e a materialidade comprovada é necessária a adoção de medidas preliminares imprescindíveis sendo a mais relevante de todas o pedido de preservação dos dados digitais perante os respectivos provedores de Internet, tendo em vista que a prova digital é extremamente volátil. Significa afirmar que uma vez apagada das plataformas dos provedores não há como recuperá-la. A coleta da prova também pode ser feita, a depender do meio empregado para a prática do crime, com a utilização de ferramentas forenses específicas.

A investigação criminal que permeia o crime cibernético, portanto, difere em vários pontos das investigações dos demais crimes, em especial, no que pertine à coleta da prova digital e respectiva cadeia de custódia.

A recente alteração legislativa ocorrida no Código de Processo Penal (Incluída pela Lei n° 13.964, de 2019) passou a tratar de forma expressa e exclusiva da "cadeia de custódia" no art.158-A e seguintes, com a finalidade de assegurar uma sequência descritiva, lógica e legal da instrução penal não se referindo, contudo, à prova digital *coletada em provedores de Internet*, motivo pelo qual se faz necessário o uso da interpretação teleológica[3] adequando a norma processual atual aos procedimentos adotados na seara cibernética.

3 Já a interpretação lógica ou teleológica busca a vontade do legislador, atendendo-se aos seus fins e a sua posição dentro do ordenamento jurídico, sempre procurando a finalidade para a qual a lei foi editada. Havendo conflito entre os tipos de interpretação, a teleológica deverá prevalecer sobre a literal, de modo a favorecer uma visão mais humana e finalística da lei. Disponível em <https://mariedeclercq.jusbrasil.com.br/artigos/151946136/a-interpretacãoda-lei-processual-penal> Acesso em 21 de abril de 2021.

Cabe consignar que a prova/vestígio digital subdivide-se em *vestígio digital com suporte físico* (consistente em todo e qualquer vestígio digital que esteja armazenado em um suporte físico identificável - *Pen Drive*, HD, *smartphone*, etc) e *vestígio digital sem suporte físico* (consiste em todo e qualquer vestígio digital que não esteja vinculado diretamente a um suporte físico, como por exemplo, os dados fornecidos diretamente pelos Provedores de Aplicação/Conexão - *Facebook, Instagram, WhatsApp,etc*), sendo que estes últimas não foram tratados pelo legislador processual penal brasileiro.

A própria norma legal trouxe o conceito expresso da cadeia de custódia, no art.158-A do Código de Processo Penal considerando o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte:

> Art. 158-A. Considera-se cadeia de custódia o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vitimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento ate o descarte. (Incluído pela Lei 11° 13.964, de 2019)

Há que se ponderar, contudo, que os estados brasileiros possuem diferentes estruturas administrativas, tanto das Policias Judiciárias, quanto dos Ministérios Públicos, ou seja, não há como impor, sob forma de obrigatoriedade legal, o cumprimento *ipsi literis,* de todas previsões legais pertinentes à cadeia de custódia, atualmente descritas na norma processual, sob pena de entender-se que eventual descumprimento de quaisquer dos dispositivos legais que tratam do tema ensejam nulidade da prova coletada, interpretação restritiva e não razoável, totalmente afastada da finalidade maior da norma.

Desta feita, não há dúvida de que o melhor entendimento para leitura da norma processual que trata da cadeia de custódia seria ter por exemplificativos os dispositivos ali elencados priorizando a finalidade real da norma e o objetivo do legislador, qual seja, assegurar uma sequência descritiva, lógica e legal da instrução penal, resguardando a prova como

um todo e evitando nulidades posteriores em respeito ao devido processo legal, ampla defesa e contraditório.

Logo, a ocorrência de meras irregularidades, ainda mais isoladas, não pode significar o descarte automático da prova sendo necessária a apuração do caso concreto a fim de verificar se aquelas irregularidades de natureza formal produziram efeitos sobre a prestabilidade ou não da fonte e/ou do meio de prova comprometendo a credibilidade destas.

O legislador ao inserir no Código de Processo Penal um capítulo específico sobre cadeia de custódia não tratou expressamente dos vestígios digitais *sem suporte físico*, no entanto, deve ser esta também a norma a ser aplicada para o tratamento das *provas digitais coletadas em provedores de Internet* primando por resguardar os indícios probatórios, ainda que a norma processual não seja aplicada de forma literal.

O Art. 158-B do Código de Processo Penal, dispõe sobre as etapas da cadeia de custódia, vejamos:

> Art. 158-B A cadeia de custódia compreende o rastreamento do vestígio nas seguintes etapas:
>
> I - **reconhecimento:** ato de distinguir um elemento como de potencial interesse para a produção da prova pericial;
>
> II - **isolamento:** ato de evitar que se altere o estado das coisas, devendo isolar e preservar o ambiente imediato, mediato e relacionado aos vestígios e local de crime;
>
> III - **fixação:** descrição detalhada do vestígio conforme se encontra no local de crime ou no corpo de delito, e a sua posição na área de exames, podendo ser ilustrada por fotografias, filmagens ou croqui, sendo indispensável a sua descrição no laudo pericial produzido pelo perito responsável pelo atendimento;
>
> IV - **coleta:** ato de recolher o vestígio que será submetido a análise pericial, respeitando suas características e natureza;
>
> V - **acondicionamento:** procedimento por meio do qual cada vestígio coletado e embalado de forma individualizada, de acordo com suas características físicas, químicas e biológicas, para posterior analise, com anotação da data, hora e nome de quem realizou a coleta e o acondicionamento;

> VI - **transporte:** ato de transferir o vestígio de um local para o outro, utilizando as condições adequadas (embalagens, veículos, temperatura, entre outras), de modo a garantir a manutenção de suas características originais, bem como o controle de sua posse;
>
> VII - **recebimento:** ato formal de transferência da posse do vestígio, que deve ser documentado com, no mínimo, informações referentes ao número de procedimento e unidade de polícia judiciária relacionada, local de origem, nome de quem transportou o vestígio, código de rastreamento, natureza do exame, tipo do vestígio, protocolo, assinatura e identificação de quem o recebeu;
>
> VIII - **processamento:** exame pericial em si, manipulação do vestígio de acordo com a metodologia adequada as suas características biológicas, físicas e químicas, a fim de se obter o resultado desejado, que devera ser formalizado em laudo produzido por perito;
>
> IX - **armazenamento:** procedimento referente a guarda, em condições adequadas, do material a ser processado, guardado para realização de contraperícia, descartado ou transportado, com vinculação ao número do laudo correspondente;
>
> X - **descarte:** procedimento referente à liberação do vestígio, respeitando a legislação vigente e, quando pertinente, mediante autorização judicial. (grifos nossos)

As etapas retromencionadas, da forma como previstas, no entanto, impossibilitam a aplicação direta às provas digitais *sem suporte físico*, ou seja, *aquelas coletadas nos provedores de Internet,* sendo necessária a adoção de procedimentos similares àqueles expressamente previstos nos dispositivos processuais penais que tratam do tema permitindo a manutenção da cadeia de custódia mediante a interpretação teleológica da norma processual.

Nesse sentido, tratando-se de prova digital coletada em provedores de Internet*,* é possível admitir o *reconhecimento* como sendo a indicação pela autoridade, ao provedor de Internet, das contas de potencial interesse; o *isolamento* como sendo a adoção de medidas pelo provedor de Internet para evitar alteração dos dados solicitados pela autoridade; a *coleta* como o ato pelo provedor de Internet de recolher o vestígio; o *armazenamento* como o procedimento referente à guarda segura do material encaminhado

pelo provedor de Internet, e, por fim, o *descarte* como sendo o procedimento referente à desobrigação do provedor de Internet em manter a guarda e preservação de dados determinados.

Nota-se que a interpretação da norma processual com aplicação à prova digital coletada em provedores de Internet, na forma supracitada, respeita os princípios norteadores da cadeia de custódia, e, consequentemente, a *mens legis,* preservando a real intenção do legislador processual quando da criação do capítulo atinente à cadeia de custódia processual penal.

Outro ponto desafiador na investigação cibernética e o uso da *Deep Web* e da *Dark Web*[4], mecanismos ardilosos, utilizados por usuários das redes sociais, que contribuem de forma significativa para o aumento da utilização da Internet para práticas criminosas. Fóruns oferecendo armas, documentos falsificados e pornografia infantil são facilmente encontrados nas páginas da *Deep Web e Dark Web* tornando-se campo fértil para a ação de criminosos sob o manto da obscuridade.

Apesar dessas redes de anonimato aparentarem ser "terra sem lei" não estão imunes às investigações pois não obstante a dificuldade e complexidade da instauração e prosseguimento de procedimentos investigatórios dessa natureza, autoridades investigativas vêm alcançando êxito na identificação de autoria e prova da materialidade em crimes cometidos nas referidas camadas da Internet, como o FBI[5] -Departamento Federal de Investigação dos EUA, o Ministério Publico Federal e a Polícia Federal[6].

4 Um site da *deep web* não tem seu conteúdo disponibilizado em mecanismos de pesquisa, e, portanto, não pode ser encontrado, exceto por quem conheça o endereço do site. A *"dark web"* consiste em sites que existem primariamente em redes an6nimas e que necessitam de programas especiais. Há outros sites que existem exclusivamente na "dark web" e não podem ser acessados sem o uso de programas como Tor, P2P e Freenet. Disponível em: <http://g1.globo.com/tecnologia/blog/segurança-digital/postideep-weboqueee-como-funciona-g1-explica.htm>. Acesso em: 28 de maio de 2024. Disponível em: <https://olhardigital.com.br/2019/03/27/noticias/tbi-apreende-us-4-5-milhões-em-criptomoeda-em-comercios ilegais-na-dark-web/>. Acesso em: 28 de maio de 2024.

5 Disponível em: <https://olhardigital.com.br/2019/03/27/noticias/tbi-apreende-us-4-5-milhões-em-criptomoeda-em-comercios ilegais-na-dark-web/>. Acesso em 28 de maio de 2024.

6 A operação DARK.NET consistiu na primeira investigação realizada na *deep web,* no Brasil, com o objetivo de identificar usuários da rede Tor *(The Onion Router)* que a utilizavam para trafegar pomografia infantil. Uma das características fundamentais desse trabalho e que toda a materialidade do crime de compartilhamento de fotos e vídeos de pornografia infantil foi obtido em um local que nunca tinha sido objeto de investigação no Brasil, qual seja, a *deep web,* inédito tanto para o Ministério Publico Federal, como para o Judiciário e também a Autoridade Policial, que foi quem criou a ferramenta.

A *Deep Web,* ou Internet profunda, é parte da Internet fechada usada para comunicações e troca de arquivos de forma anônima e normalmente e acessada através de aplicativos da rede TOR[7](The Onion Router). A complexidade para identificar os autores das práticas criminosas decorre do fato de ser a rede TOR uma "rede de túneis" por onde a informação percorre, modificando continuamente o número de IP[8], desde o emissor até o receptor, tomando assim anônima a identidade do IP de origem.

A *Dark Web* é uma pequena parcela da *Deep Web* também composta por sites e redes que não são indexados pelos mecanismos de busca. Porém, diferente da primeira, a quase totalidade dos domínios nesta parte da *web* são voltados para práticas criminosas. Os termos "*Deep Web"* e *"Dark Web",* portanto, não são sinônimos, mas ambas as redes são inacessíveis pelos mecanismos de busca e compostas de sites e conteúdos que não são públicos por diversos motivos, como acesso pago ou questões de privacidade.

Em uma investigação cibernética, a identificação do IP e a quebra do sigilo de seus dados cadastrais permitem identificar o usuário do serviço prestado pelo provedor de conexão. Insta salientar, entretanto, que muitas vezes o usuário do serviço de Internet é pessoa diversa daquele indivíduo que está sendo investigado. Isto porque não é raro que um único IP seja compartilhado por um número de pessoas de uma mesma família, um mesmo condomínio ou no mesmo local de trabalho, tomando-se mister o aprofundamento das investigações com a finalidade de identificar com segurança o verdadeiro autor do crime aplicando-lhe as medidas cautelares cabíveis, seja a busca e apreensão ou prisões, preventiva ou temporária.

Aos demais desafios, até aqui expostos, some-se a demora dos provedores de conexão à Internet em atualizar seus sistemas de

7 A rede TOR (The Onion Route) e uma rede que cria uma cadeia de roteadores (encaminha comunicações de rede) que permite que o usuário navegue de uma forma anônima, utilizando comunicações criptografadas de chaves pública e privada. Disponível em <https://noticias.r7.com/sao-paulo/deep-web-como-a-parte-obscura-da-Internet-e usada-para-crimes-16O3201ç> - Acesso em: 28 de maio de 2024.

8 O IP (Internet Protocol), e um protocolo usado para identificar dispositivos ou conexões. Cada aparelho ou dispositivo possui um IP fixo, enquanto a conexão com a Internet gera IPs dinâmicos, também conhecido como IP externo. O IP externo e a identificação gerada a partir da conexão do seu dispositivo com uma rede. Assim como o CPF, cada equipamento gera um protocolo de identificação diferente quando conectado a Internet, logo, não existe duplicidade de IPs entre redes e dispositivos. O IP interno identifica o dispositivo, e não a conexão entre ele e uma rede externa. Esse protocolo e importante para manutenção de impressoras, computadores e servidores, por exemplo, dentro de empresas ou para outros reparos. Disponível em: <https://canaltech.com.br/internet/o-que-e-ip/>. Acesso em: 28 de maio de 2024.

identificação de usuários da rede mundial de computadores, dificultando, em demasia, o trabalho das autoridades encarregadas de investigar crimes cibernéticos, isto porque

> Alguns provedores, por várias questões, não querem fazer a migração. [...] eles pegam um endereço de IP e compartilham [entre vários clientes]. Já pegamos um único IP sendo usado por 1.020 aparelhos. Como vamos chegar à conexão?" [...]. "É como se tivéssemos uma autopista com mil veículos, todos da mesma cor e com uma mesma placa. [Por isso] alguns abusadores e exploradores sexuais deixaram de ser identificados.[…] Isso não afeta só crime de abuso e exploração sexual infantil. Afeta fraudes eletrônicas, crimes eleitorais, o que quer que seja que exija a identificação do responsável. [9]

O obstáculo se impõe em razão da resistência das empresas de provedores de Internet em realizar os investimentos necessários para migrarem da tecnologia IPv4 para a IPv6 - protocolo de *Internet* (IP). O IPv6 surge no ano de 2012, como medida necessária para solucionar o iminente esgotamento dos "endereços" numéricos (Ips) identificadores de cada dispositivo eletrônico conectado à rede mundial de computadores.

O IPv4 foi criado no inicio da década de 1980, apresentando-se com "endereços" Ips que continham 32 bits suportando cerca de 4,30 bilhões de IPs em todo o mundo. São exatamente as combinações numéricas que identificam um IP e permitem a conexão dos equipamentos em rede, ou seja, para acessar à Internet, o usuário, necessariamente, utiliza um equipamento com um número de IP autenticado. No entanto, com a popularização da Internet e a "Internet das coisas", o número de endereços disponíveis no protocolo IPv4 sofreu drástica redução motivando a criação do IPv6 que por possuir 128 bits, possibilita um número muito maior de combinações numéricas.

Ocorre que, com o esgotamento do antigo protocolo (IPV4) muitos provedores de Internet que ainda não migraram para o protocolo IPv6 passaram a atribuir um mesmo IP a mais de um usuário impossibilitando, com tal procedimento, a individualização da conduta, e, consequentemente,

9 Alessandro Barreto - Coordenador do Laboratório de Inteligência Cibernética do Ministério da Justiça e Segurança Pública. Disponível em <https://agenciabrasil.ebc.com.br/geral/noticia/2019-09/acao-de-provedores-dificulta-identificacao-de-criminosos-ciberneticos>. Acesso em 28 de maio de 2024.

a identificação da autoria criminosa, afetando de forma drástica, o curso das investigações criminais.

O *Network Address Translation* - NAT, é o sistema utilizado pela maioria dos provedores de conexão que permite o "compartilhamento" de um IP único entre diversos computadores como forma de mitigar o esgotamento do IPv4 até a implementação completa do IPv6.

O NAT adiciona um dado a mais conjugado com o endereço IP de conexão identificado, a porta lógica, que permite que o provedor de conexão indique qual cliente estaria utilizando um determinado IP compartilhado para se conectar à rede externa de forma a rotear apropriadamente os dados. Destarte, a porta lógica associada ao endereço IP permite identificar de forma individualizada o usuário do serviço.

Entretanto, a falta de registros de conexão com a porta lógica por parte dos provedores de aplicação acaba por impossibilitar a junção destes dados impossibilitando a identificação de plano dos criminosos, sendo necessário o aprofundamento das investigações na tentativa de descobrir a autoria do delito penal praticado, somando-se o dado digital (falho) fornecido pelas empresas, com as demais provas produzidas.

Sobre o esgotamento do IPv4:

> A falta de IPs disponíveis para conexões à internet e a necessidade de investimento para a implementação do IPv6 fez com que as operadoras de telefonia passassem a utilizar o NAT-44: um sistema no qual um mesmo IP passa a ser compartilhado por muitos usuários ao mesmo tempo. Seria mais ou menos como utilizar um filtro de linha, com diferentes usuários se plugando nas tomadas/entradas de um mesmo IP. Para identificar o usuário seria necessário que cada "tomada" fosse identificada, isto é, cada porta lógica precisaria ser guardada tanto pelos provedores de conexão à internet, quanto pelos provedores de aplicações, além do número de IP, data e hora, o que demanda mais investimento. A consequência disso é que, embora os provedores de conexão de internet estejam avançando na implementação do IPv6, muitas investigações que dependiam somente da informação referente àquelas conexões efetuadas através do NAT 44 acabaram ficando sem solução.[10]

10 Disponível em <https://escola.mpu.mp.br/plataforma-aprender/acervo-educacional/conteudo/201cinvestigacao-de-crimes-ciberneticos/texto-complementar-aula-1_crimes-ciberneticos-e-governanca_revisao-final-pa-

Em decisão proferida pela Terceira Turma do Superior Tribunal de Justiça (STJ), determinou-se a um provedor de aplicação de Internet que fornecesse à operadora de telefonia os dados da porta lógica associada a um endereço do tipo IPv4 para a apuração dos dados do responsável por oferecer indevidamente um plano de telefonia:

> RECURSO ESPECIAL. CIVIL E PROCESSUAL CIVIL. AÇÃO DE OBRIGAÇÃO DE FAZER. PROVEDOR DE APLICAÇÃO. IDENTIFICAÇÃO DO DISPOSITIVO UTILIZADO PARA ACESSO A APLICAÇÃO. INDICAÇÃO DO ENDEREÇO IP E PORTA LÓGICA DE ORIGEM. INTERPRETAÇÃO TELEOLÓGICA DOS ARTS. 5°, VII, E 15 DA LEI Nº. 12.965/2014. RECURSO ESPECIAL PROVIDO. 1. O recurso especial debate a extensão de obrigação do provedor de aplicações de guarda e fornecimento do endereço IP de terceiro responsável pela disponibilização de conteúdo ilícito as informações acerca da porta 1ógica de origem associada ao IP. 2. A previsão legal de guarda e fornecimento dos dados de acesso de conexão e aplicações foi distribuída pela Lei n. 12.965/2014 entre os provedores de conexão e os provedores de aplicações, em observância aos direitos a intimidade e a privacidade. 3. Cabe aos provedores de aplicações a manutenção dos registros dos dados de acesso a aplicação, entre os quais se inclui o endereço IP, nos termos dos arts. 15 combinado com o art. 5°, VIII, da Lei n. 12.965/2014, os quais poderão vir a ser fornecidos por meio de ordem judicial. 4. A obrigatoriedade de fornecimento dos dados de acesso decorre da necessidade de balanceamento entre o direito a privacidade e o direito de terceiros, cujas esferas jurídicas tenham sido aviltadas, a identificação do autor da conduta ilícita. 5. Os endereços de IP são os dados essenciais para identificação do dispositivo utilizado para acesso a Internet e as aplicações. 6. A versão 4 dos IPs (IPv4), em razão da expansão e do crescimento da Internet, esgotou sua capacidade de utilização individualizada e se encontra em fase de transição para a versão 6 (IPv6), fase esta em que foi admitido o compartilhamento dos endereços IPv4 como solução temporária. 7. Nessa fase de compartilhamento do IP, a individualização da navegação na Internet passa a ser intrinsecamente dependente da porta 1ógica de origem, ate a migração para o IPv6. 8. A revelação das portas 1ógicas de origem consubstancia simples desdobramento lógico do pedido de identificação do usuário por IP. 9.

no-pra-manga_180621.pdf>. Acesso em: 28 de maio de 2024.

> Recurso especial provido. (RECURSO ESPECIAL Nº 1.784.156 - SP (2018/0322140-0) - Ministro Marco Aurélio Bellizze - Brasília, 05 de novembro de 2019 (data do julgamento) -DJe: 21/11/2019

Importante frisar, contudo, que a decisão retro mencionada não afasta a obrigação dos provedores de conexão em fornecer os dados cadastrais dos usuários vinculados a determinado endereço IPv4, mas, tão somente, reportou-se à obrigatoriedade dos provedores de aplicação em armazenarem e fornecerem os dados pertinentes às respectivas portas lógicas com a finalidade de identificar o usuário do serviço prestado.

Diante disto, os provedores de conexão não pode negar o fornecimento de dados cadastrais de usuários de IPv4 ao fundamento de impossibilidade de individualização do utilizador daquele registro de conexão em decorrência da ausência do dado da porta lógica associada. Ou seja, ainda que não haja o fornecimento do dado da porta lógica pelo provedor de aplicação, os nomes de todos os usuários daquele IPv4, na data e hora informadas, deverão ser fornecidos pelos provedores de conexão à autoridade que investiga cabendo a esta a análise da massa de dados gerada a fim de identificar dentre os usuários de um mesmo IP, o suposto autor do crime, o que será constatado mediante o somatório de outras provas já produzidas.

A promulgação do Marco Civil da Internet significou grande avanço na busca da regulamentação das condutas praticadas no meio digital, e, principalmente, no combate aos crimes virtuais e aos crimes comuns, cujas provas de autoria e/ou materialidade encontram-se em meio virtual, haja vista que a referida norma, hoje acrescida da Convenção de Budapeste, traz mecanismos eficazes e relevantes à investigação criminal, conforme se observará no tópico a seguir.

2. A CONVENÇÃO DE BUDAPESTE E A LEI DO MARCO CIVIL DA INTERNET COMO INSTRUMENTOS DE INVESTIGAÇÃO

A Convenção de Budapeste sobre Cibercriminalidade (CETS 185) encontra-se vigente na Europa desde 1º de julho de 2004 e foi aprovada no Brasil pelo Decreto Legislativo 37/2021 passando a vigorar em 1º de

março de 2023, quando findo o processo de adesão. Após a promulgação da Convenção de Budapeste, pelo Decreto 11.491/2023, o texto passou a ter vigência interna a partir de 13 de abril de 2023, quando o tratado foi publicado no Diário Oficial da União.

É instrumento internacional vinculante e de orientação a qualquer país que pretenda desenvolver legislação nacional abrangente contra o cibercrime. O objetivo do indigitado documento internacional é aplicar uma política penal comum para proteger a sociedade contra os crimes cibernéticos, entre outras formas, mediante a adoção de uma legislação adequada, fomentando, para tanto, a cooperação internacional entre os Estados-membros do tratado.

Inicialmente a Convenção de Budapeste foi projetada para definir e harmonizar as normas de direito penal e processual penal referentes a crimes cibernéticos cometidos dentro da jurisdição dos Estados-membros do Conselho da Europa, contudo, a partir do ano de 2013 também Estados não membros passaram a ser convidados, sendo o Brasil um destes países, cujo convite foi formalizado em 2019. Agora, signatário, o Brasil se une ao círculo internacional composto por Estados-membros do Conselho da Europa e por Estados não membros.

O preâmbulo da Convenção de Budapeste prioriza "uma política criminal comum, com o objetivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adoção de legislação adequada e da melhoria da cooperação internacional" e reconhece "a necessidade de uma cooperação entre os Estados e a indústria privada".

A Convenção de Budapeste traz como principal destaque a definição dos crimes cibernéticos, tipificando-os como infrações contra sistemas e dados informáticos, infrações relacionadas com computadores, infrações relacionadas com o conteúdo, pornografia infantil, infrações relacionadas com a violação de direitos autorais.

Além da importância da promulgação da Convenção de Budapeste no ordenamento jurídico brasileiro mister ressaltar a relevância da Lei 12.965/14 - Marco Civil da *Internet,* promulgada com o objetivo de suprir a carência por um marco equivalente na seara criminal que tratasse da

delimitação de parâmetros de persecução penal para tais crimes que em razão de sua natureza transcendem as fronteiras geográficas.

> Uma das funções do Marco Civil brasileiro foi gerar segurança jurídica, de modo a oferecer normatização específica ao Poder Judiciário para resolução de questões que envolvam internet e tecnologia da informação, de modo a se evitar decisões contraditórias sobre temas que envolvam o mesmo assunto. JESUS, Damásio de; MILAGRE, José Antônio. Marco Civil da internet: comentários à Lei n. 12.965/2014. São Paulo: Saraiva, 2014, p. 18.

Um dos pontos relevantes a ser tratado nesta oportunidade, é exatamente a aplicação do Marco Civil da Internet e da Convenção de Budapeste, em harmonia, entrelaçados, como instrumentos de persecução penal já que a mera assunção de obrigações internacionais para o combate ao cibercrime não seria suficiente, tornando-se necessária a adoção de medidas internas em matéria penal e processual penal para torná-las efetivas.

A Convenção de Budapeste descreve em seu texto condutas penais variadas, consideradas relevantes cuja finalidade é alcançar o maior número de Estados no combate à criminalidade cibernética:

> Por esse motivo, variadas são as condutas trazidas pela Convenção de Budapeste a serem criminalizadas pelos Estados-parte, desde as que surgiram na era digital até as já existentes, mas que passaram a utilizar a Internet como meio de cometimento: acesso ilegal, interceptação ilícita, violação de dados, obstrução ou impedimento de acesso, uso indevido de aparelhagem, falsificação e fraude informática, pornografia infantil e violação de direitos autorais ou correlatos. Buscou-se descrever condutas consideradas penalmente relevantes, eleitas como as mais sensíveis à época, para auxiliar o combate à criminalidade cibernética e evitar abusos decorrentes da legislação menos rigorosa de um Estado, que impactam outros países. (…) Deve haver cuidado com a tipificação de novas condutas trazidas pela Convenção, para não resultar em sobreposição com os tipos penais já previstos na legislação brasileira ou excesso punitivo. A análise do bem jurídico, a tipificação clara e a previsão de penas proporcionais são etapas fundamentais e que demandam discussão com certo nível de maturidade, para que não se torne mais uma norma penal ineficaz, a

> trazer insegurança jurídica e a permitir arbitrariedades no exercício do poder estatal. (MURATA e TORRES, 2023, p.14)

No ordenamento jurídico-penal brasileiro é possível citar a Lei 12.737 de 2012 ("Lei Carolina Dieckmann") que inseriu no Código Penal o delito de "invasão de dispositivo informático" entre outros crimes virtuais e a Lei 14.155 de 2021[11] que modificou e incluiu alguns dispositivos do Código Penal promovendo alterações com relação aos crimes de invasão de dispositivos informáticos, furto mediante fraude eletrônica, estelionato mediante fraude eletrônica, dentre outras questões relevantes.

A Lei 14.132 de 2021 inseriu no Código Penal o art. 147-A, denominado "crime de perseguição" ou C*yberstalking*, que tem como bem jurídico tutelado, a liberdade individual, tratando-se de delitos cometidos no âmbito da Internet, de forma reiterada, com a finalidade de constranger a vítima por meio da invasão da privacidade.

A promulgação da Convenção de Budapeste e a inserção de seu texto jurídico no ordenamento jurídico passou a proporcionar às autoridades brasileiras acesso mais ágil às provas eletrônicas sob jurisdição estrangeira além de tornar mais efetiva a cooperação jurídica internacional indicando também parâmetros para o armazenamento de dados sensíveis e busca e apreensão de dados informáticos.

Importante inovação trazida pela Convenção de Budapeste no combate aos crimes cibernéticos são as medidas de cooperação jurídica internacional fixadas para obtenção de provas digitais, escritas de forma clara nos arts. 23 a 35, verdadeira "troca" e auxílio entre os Estados signatários o que para o Brasil, sem dúvida, tornará muito mais eficiente a busca dos dados digitais quando estes estiverem fora do país:

> Além de estimular os laços com outros Estados, a ratificação de um tratado com dispositivos de cooperação sobre provas digitais era há tempos devida, já que tais provas, pelas suas características específicas (volatilidade, ubiquidade e dispersão), diferem das provas corpóreas e requerem procedimentos cooperacionais específicos para a sua

11 Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato.

> obtenção (BADARÓ, 2021, apud MURATA e TORRES, 2023, p.15).

Não são raras as vezes em que no curso de uma investigação criminal constata-se que determinados dados digitas da pessoa investigada encontram-se armazenados em provedores localizados em outro Estado e sem sede ou filial no Brasil.

Nesse caso, não obstante o usuário dos serviço encontrar-se situado no Brasil, seus dados digitais estão alocados em provedores fora do país sendo acessados de forma remota de qualquer local do mundo já que estariam armazenados em nuvem. A dificuldade de acesso aos dados digitais pelas autoridades em casos como estes era habitual, e, em contrapartida, ao investigado era possível deletar seus dados digitais a qualquer tempo de forma remota enquanto não fossem preservados.

Antes da promulgação da Convenção de Budapeste, esta situação fática, alhures narrada, na qual os dados digitais encontravam-se armazenados em Estado diverso tornava-se um entrave na maioria das vezes intransponível ao prosseguimento das investigações criminais em curso, haja vista que os provedores localizados em outros países recusavam-se a fornecer os dados diretamente às autoridades brasileiras.

Um dos principais objetivos da Convenção de Budapeste é fomentar e efetivar a cooperação jurídica internacional probatória no combate aos crimes cibernéticos, e, para tanto, este instrumento de cooperação traz importantes procedimentos cautelares[12] específicos para obtenção de provas digitais, dentre estes, pedido de busca, acesso, apreensão, guarda ou revelação de dados armazenados por meio de computador, pedido de interceptação de dados de tráfego em tempo real, pedido de interceptação ou gravação em tempo real, entre outras medidas cooperacionais.

A preservação dos dados informáticos é medida de extrema relevância nas investigações criminais ora tratadas. Tal se afirma, uma vez que essa

12 A Convenção de Budapeste prevê nos seus artigos instrumentos que facilitam o acesso o pedido de busca, acesso, apreensão, guarda ou a revelação de dados armazenados por meio de computador (art. 31); pedido de interceptação de dados de tráfego em tempo real (art. 33); e pedido de interceptação ou gravação em tempo real do conteúdo de comunicações específicas transmitidas por meio de um sistema de computador (art. 34), acesso transfronteiriço a dados armazenados em computador, sem a necessidade de cooperação jurídica internacional: quando houver consentimento daquele com autoridade legal para revelar os dados ou quando os dados estiverem em sistema de acesso público (art. 32); o sistema de plantão 24 por 7, em que cada Estado indica um órgão de contato para, entre outros, receber comunicações urgentes de pedidos de prova digitais (art. 35) – no Brasil este órgão de contato é a Polícia Federal.

providência resguarda os dados investigados, "congelando-os" para posterior utilização em ação penal, quando então, a depender da natureza do dado preservado[13], será necessária, ou não, a autorização judicial para o acesso àqueles.

Note-se, ainda, que os prazos legais e obrigatórios para preservação/ guarda dos dados/ provas digitais pelos provedores de Internet[14] encontram-se previstos na Lei do Marco Civil da *Internet* (Lei 12.965/14), quais sejam, 06 (seis) meses para provedores de aplicação e 01 (um) ano para provedores de conexão, vejamos:

> **Da Guarda de Registros de Conexão**
>
> Art. 13. Na provisão de conexão à *Internet,* cabe ao administrador de sistema autónomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento. (grifo nosso)
>
> **Da Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Aplicações**
>
> Art. 15. O provedor de aplicações de *Internet* constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos devera manter os respectivos registros de acesso a aplicações de *Internet,* sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento. (grifo nosso)

Verifica-se, portanto, que uma vez decorrido o lapso temporal legal previsto no Marco Civil não estão os provedores de Internet obrigados a guardar os registros de conexão ou registros de acesso à aplicação de Internet, salvo se houver pedido judicial nesse sentido para preservação/

13 Os dados cadastrais podem ser requisitados diretamente pelo Ministério Público ou pela Polícia Judiciária, no curso de uma investigação criminal. Os dados de tráfego e conexão também podem ser acessados, contudo, apenas mediante prévia autorização judicial, no curso de uma investigação civil, criminal ou administrativa, ou para a instrução de ação cível, trabalhista ou penal. Os dados de conteúdo, dotados de maior proteção, só podem ser acessados por ordem judicial, exclusivamente para fins de persecução criminal, nos termos da Lei 9.296/1996 ou do Marco Civil da Internet.

14 Provedor de Aplicação de Internet – pessoa jurídica que fornece conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à Internet, a grosso modo seriam os provedores de serviços on line - fornecimento de dados pessoais/cadastrais, conteúdo de comunicações e registros de acesso a aplicações de Internet (IPs utilizados para respectivos acessos); Provedor de Conexão de Internet – pessoa jurídica fornecedora de serviços de acesso à Internet-fornecimento de dados cadastrais e registros de conexões - IPs e portas 1ógicas.

guarda de dados por prazo superior àquele legalmente previsto, conforme se denota na norma legal abaixo transcrita:

> **Da Guarda de Registros de Conexão**
>
> Art.13. Na provisão de conexão à Internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.
>
> [...]
>
> § 2° A autoridade policial ou administrativa ou o Ministério Publico **poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no caput.** (grifo nosso)
>
> **Da Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Aplicações**
>
> Art. 15. O provedor de aplicações de Internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de Internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.
>
> [...]
>
> § 2° A autoridade policial ou administrativa ou o Ministério Publico **poderão requerer cautelarmente a qualquer provedor de aplicações de Internet que os registros de acesso a aplicações de Internet sejam guardados, inclusive por prazo superior ao previsto no caput,** observado o disposto nos §§ 3° e 4° do art. 13. (grifo nosso)

É dizer que a preservação dos dados digitais a pedido da autoridade aos provedores de Internet garante, desde que adotadas as medidas administrativas e legais necessárias, a dilação do prazo de guarda dos registros por período superior àquele previsto em lei, possibilitando a guarda até ao final da investigação ou da instrução criminal. Sendo assim, ainda que o investigado ou o próprio provedor de Internet, venham a apagar os dados digitais de determinada conta, estes permanecerão incólumes, preservando o lastro probatório.

O questionamento a ser feito, portanto, seria: autoridades policiais e promotores de justiça estão autorizados legalmente a solicitar aos provedores de Internet e equiparados a preservação de todo e qualquer dado digital sem autorização judicial?

Apesar de existência de decisão do Supremo Tribunal Federal anulando provas obtidas a partir de dados preservados em contas da Internet sem autorização judicial fato é que o Marco Civil da Internet não exige autorização judicial para o pedido de preservação de dados, apenas o fazendo quanto à disponibilização destes dados, ressalvado os dados cadastrais, que podem ser requisitados independentemente de ordem judicial:

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de Internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
>
> § 1º O provedor responsável pela guarda **somente será obrigado a disponibilizar os registros mencionados no caput,** de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, **mediante ordem judicial**, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º .
>
> § 2º **O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial**, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º .
>
> **§ 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição**. (grifo nosso)

A leitura do dispositivo legal retro, enseja a seguinte conclusão lógica: a *disponibilização* dos dados digitais apenas poderá ser efetuada pelos provedores de Internet mediante *autorização judicial***,** mas, em contrapartida, o *acesso a dados cadastrais* que informem qualificação pessoal, filiação e endereço *não são abrangidos pela exigência de ordem judicial* sendo possível

obtê-los mediante mera requisição pelas autoridades administrativa que detenham competência legal.

Extrai-se, ainda, da leitura do referido dispositivo legal a conclusão de que a autorização judicial exigida por lei apenas é direcionada à *disponibilização* dos registros de conexão e de acesso a aplicações de Internet, bem como de dados pessoais e do conteúdo de comunicações privadas, não havendo a exigência judicial com relação à mera guarda/preservação dos ditos dados pelos provedores de Internet.

De fato, não faria sentido impor à guarda/preservação dos dados informáticos à morosidade que naturalmente decorre de um processo judicial uma vez que tal demora, por certo, colocaria em risco a manutenção da prova pretendida dando fim à investigação criminal, mormente, quando essa prova for a principal.

Note-se que ao requisitar o pedido de preservação de dados informáticos/digitais diretamente ao provedor de Internet o atendimento à requisição é quase automático, garantindo que aqueles dados não sejam definitivamente deletados, seja pelo investigado, ou pelo próprio provedor de Internet em razão do decurso do lapso temporal legal para a guarda daqueles.

A *mens legis*[15], portanto, foi preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas, direitos fundamentais não violados com o mero procedimento de preservação de dados pelos provedores de Internet uma vez que difere do acesso propriamente dito aos dados preservados, estes sim, apenas fornecidos mediante ordem judicial. Quis ainda o legislador garantir a preservação da prova digital, volátil por sua natureza, não exigindo ordem judicial para fazê-lo sendo suficiente a requisição administrativa por quem tem competência legal para tanto.

A Lei do Marco Civil em consonância com a norma constitucional[16] vigente protege os dados pessoais, direitos fundamentais que não podem

15 O Art. 10. da Lei do Marco Civil expressamente dispõe que a guarda e a disponibilização dos registros de conexão e de acesso a aplicações de Internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

16 Art. 5º (…) LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais. (Incluído pela Emenda Constitucional nº 115, de 2022)

ser violados sob hipótese alguma, ressalvadas a expedição de ordem judicial. Exatamente por isto os dados digitais que ponham em risco a preservação da intimidade, da vida privada, da honra e da imagem dos usuários dos serviços de Internet não podem ser fornecidos administrativamente às autoridades investigativas. Ao revés, exige-se, para tanto, ordem judicial expressa sob pena de serem declaradas nulas as provas obtidas de forma diversa.

Se por um lado, os dados cadastrais[17] podem ser requisitados diretamente pelo Ministério Público ou pelas Polícias Judiciárias, no curso de uma investigação criminal, os dados de tráfego[18] e conexão[19] e os dados de conteúdo[20], estes últimos dotados de maior proteção, apenas serão fornecidos pelos provedores de Internet mediante ordem judicial e exclusivamente para fins de persecução criminal, nos termos da lei.

A investigação criminal cibernética enfrentava, antes mesmo da vigência da Convenção de Budapeste, além do desafio da inexistência de norma penal e processual penal específicas e a deficiência na qualificação de grande parte das autoridades que investigam, também a recusa de determinados provedores de Internet em cumprirem a legislação brasileira, notadamente quanto ao fornecimento de conteúdo de comunicação privada.

O fundamento utilizado pelos provedores de aplicação para negarem o fornecimento de conteúdo de comunicação privada era no sentido de que esses não estariam sujeitos as leis brasileiras, alegando, ainda, a obrigatoriedade de utilização de instrumentos de cooperação internacional judiciária, no caso, o MLAT *(Mutual Legal Assistance Treaty)*.

17 O §2º do art. 11 do Decreto 8.771/2016, que regulamenta a Lei do Marco Civil considera dados cadastrais: a filiação; o endereço; e a qualificação pessoal, entendida como nome, prenome, estado civil e profissão do usuário.

18 De acordo com a Convenção de Budapeste, no seu artigo 1, "dados de tráfego" significa todos os dados informáticos relacionados com uma comunicação efetuada por meio de um sistema informático, gerados por este sistema como elemento de uma cadeia de comunicação, indicando a origem da comunicação, o destino, o trajeto, a hora, a data o tamanho, a duração ou o tipo do serviço subjacente.

19 O art. 5º, V, do Marco Civil da Internet, traz a definição de dados de conexão, denominando-os de registros de conexão, como o "conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados".

20 Dados informáticos de conteúdo comunicacional, são as informações transmitidas entre usuários de Internet, no curso de uma telecomunicação, por meios telefônicos ou telemáticos, ou ainda por comunicadores e mensageiros instantâneos, criptografados ou não, protegidos pelo inciso XII do art. 5º da Constituição Federal, considerados, portanto, mais sensíveis no que tange à privacidade.

Na Ação Declaratória de Constitucionalidade (ADC) 51, a Federação das Associações das Empresas de Tecnologia da Informação (Assespro Nacional) pedia a declaração de validade do Acordo de Assistência Judiciária em Matéria Penal (MLAT, na sigla em inglês), promulgado pelo Decreto Federal 3.810/2001, usado em investigações criminais e instruções penais em curso no Brasil sobre pessoas, bens e haveres situados nos Estados Unidos. O referido acordo bilateral tratava da obtenção de conteúdo de comunicação privada sob controle de provedores de aplicativos de Internet sediados fora do país.

A tese suscitada pelos provedores de Internet na ADC 51, contudo, não se sustentava, mormente porque nos termos do artigo 11 da Lei 12.965/2014 ("Marco Civil da Internet"), e do art.18 da Convenção sobre Crimes Cibernéticos de Budapeste, a legislação brasileira deverá ser obrigatoriamente respeitada no que se refere a qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de Internet, quando pelo menos um desses atos ocorra em território nacional:

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de Internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
>
> Artigo 18 - Ordem de exibição
>
> 1. Cada Parte adotará as medidas legislativas e outras providências necessárias para dar poderes a autoridades competentes para ordenar:
>
> a. a qualquer pessoa residente em seu território a entregar dados de computador especificados, por ela controlados ou detidos, que estejam armazenados num sistema de computador ou em qualquer meio de armazenamento de dados de computador;
>
> b. a qualquer provedor de serviço que atue no território da Parte a entregar informações cadastrais de assinantes de

> tais serviços, que estejam sob a detenção ou controle do provedor.(...)

O Plenário do Supremo Tribunal Federal (STF), julgou constitucional a possibilidade de autoridades nacionais solicitarem dados diretamente a provedores de aplicação estrangeiros com sede ou representação no Brasil sem, necessariamente, seguir o procedimento do acordo celebrado entre o Brasil e os Estados Unidos.

Significa dizer que de acordo com o Supremo Tribunal Federal é possível a solicitação direta das informações/dados digitais aos provedores de Internet com fundamento na Lei do Marco Civil tendo o MLAT e Cartas Rogatórias papel meramente complementar e subsidiário:

> AÇÃO DECLARATÓRIA DE CONSTITUCIONALIDADE. NORMAS DE COOPERAÇÃO JURÍDICA INTERNACIONAL. OBTENÇÃO DE DADOS. EMPRESAS LOCALIZADAS NO EXTERIOR. DECRETO Nº 3.810/2001; ART. 237, II DO CPC; ARTS. 780 E 783 DO CPP; ART. 11 DO MARCO CIVIL DA INTERNET; ART. 18 DA CONVENÇÃO DE BUDAPESTE. CONSTITUCIONALIDADE. ADC CONHECIDA. PEDIDO JULGADO PARCIALMENTE PROCEDENTE. 1. A controvérsia constitucional veiculada na ADC é, a rigor, mais ampla do que a simples declaração de validade do uso das cartas rogatórias e dos acordos MLAT para fins de investigação criminal. O escopo da ação declaratória compreende não apenas o exame de constitucionalidade dos dispositivos invocados pelos requerentes, como também da norma prevista no art. 11 do Marco Civil da Internet e art. 18 da Convenção de Budapeste. 2. O art. 11 do Marco Civil da Internet, que encontra respaldo no art. 18 da Convenção de Budapeste, é norma específica em relação às regras gerais do MLAT. O referido dispositivo assegura a aplicação da legislação brasileira em relação a atividades de coleta, armazenamento, guarda e tratamento de registros, dados e comunicações eletrônicas ocorridas em território nacional, desde que pelo menos um dos atos ou terminais se encontrem em território nacional, mesmo que a pessoa jurídica portadora dessas informações esteja localizada ou armazene tais informações no exterior. 3. As hipóteses de requisição direta previstas no art. 11 do Marco Civil da Internet e no art. 18 da Convenção de Budapeste reafirmam os princípios da soberania e da independência nacional, concretizando o dever do Estado de proteger os

> direitos fundamentais e a segurança pública dos cidadãos brasileiros ou residentes no país. 4. Constitucionalidade dos dispositivos do MLAT, do CPC e do CPP que tratam da cooperação jurídica internacional e da emissão de cartas rogatórias, nos casos em que a atividade de comunicação ou a prestação de tais serviços não tenham ocorrido em território nacional. 5. Dispositivos que convivem com a possibilidade de solicitação direta de dados, registros e comunicações eletrônicas nas hipóteses do art. 11 do Marco Civil da Internet e do art. 18 da Convenção de Budapeste. 6. Pedido julgado parcialmente procedente para declarar a constitucionalidade dos dispositivos indicados e da possibilidade de solicitação direta de dados e comunicações eletrônicas das autoridades nacionais a empresas de tecnologia nos casos de atividades de coleta e tratamento de dados no país, de posse ou controle dos dados por empresa com representação no Brasil e de crimes cometidos por indivíduos localizados em território nacional. (ADC nº 51/DF – Plenário - Relator Ministro Gilmar Mendes – Julgamento: 23 de fevereiro de 2023 - Requerente: Federação das Associações das Empresas Brasileiras de Tecnologia da Informação - Assespro Nacional. Publicação Original [diário oficial da união de 28 de abril de 2023] (p. 1, col. 1)

Ressalte-se, ainda, que o MLAT aplicado de maneira isolada não seria eficiente para a produção das provas digitais requeridas pelas autoridades brasileiras haja vista a notória morosidade[21] no atendimento dos pleitos formulados, além das limitações impostas pela legislação norte-americana.

Note-se, ainda, que o §2°, do art.11 da Lei do Marco Civil da Internet dispõe, expressamente, que as empresas que prestam serviço ao público brasileiro ou que possuam estabelecimento no Brasil integrantes de grupo econômico de provedor de Internet com sede no exterior submetem-se à legislação brasileira quanto às operações de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de Internet.

Nos dias atuais a obtenção de dados digitais tomou-se medida imprescindível no combate à criminalidade, seja para apuração de crimes

21 Levantamento feito pelo Departamento de Recuperação de Ativos e Cooperação jurídica Internacional (DRCI), vinculado ao Ministério da Justiça, revelou que dos 108 pedidos de cooperação jurídica internacional feitos com base no acordo, apenas 18 tiveram as diligências atendidas. Disponível em: <https:/ Impf.jusbrasil.com.br/noticias/567O26633/aplicativos-com-sede-no-exterior-devem-obedecer-legislacão-brasileira-defende-mpf?ref=feed>. Acesso em: 28 de maio de 2024.

cibernéticos propriamente ditos, ou para a investigação de crimes comuns não praticados com a utilização de sistema informático. A prova digital "*pode ser entendida como a demonstração de um fato ocorrido nos meios digitais*" (RODRIGUES; TAMER, 2021, p. 291).

A coleta da prova digital deve ser realizada pelos provedores de Internet de forma efetiva e célere, sob pena de haver perda desse lastro probatório, frágil e volátil por sua natureza. Para fixação da legislação a ser aplicada deve ser considerado o território do usuário e não o local da sede da empresa dos provedores de Internet, como pretendiam estes últimos.

Insta salientar que os dados e comunicações requisitados aos provedores de Internet provêm de usuários brasileiros, colhidos em território nacional, para apuração de crimes de competência da Justiça Brasileira. Some-se a isto o fato de que referidos dados são coletados durante a prestação de serviço a brasileiros justificando assim a aplicação e prevalência da jurisdição brasileira, ainda que haja produção de efeitos em outros países onde estejam armazenados os dados solicitados. Isto porque:

> De fato, a sociedade da informação e da comunicação é um "mundo" com intenso fluxo de informações, que está em veloz e permanente mudança e em que o conhecimento é flexível, fluido e sempre em expansão; as noções existentes sobre território foram relativizadas, pois superadas as barreiras que o espaço, assim como o tempo, impunham à comunicação entre as pessoas, notadamente as ausentes. (KIST, Dario José, 2024, p.25)[22]

A coleta de provas digitais é um processo rígido e específico que tem por objetivo garantir que as evidências eletrônicas/digitais sejam utilizadas de forma válida e eficaz para alcançar autoria e materialidade dos crimes. A integridade dessas provas é essencial para assegurar que elas sejam admitidas e não tenham seu valor probatório questionado em juízo, mantendo íntegra o lastro probatório produzido no curso da investigação criminal.

22 KIST, Dario José. Prova Digital no Processo Penal. Ed. Mizuno, 2024.

CONCLUSÃO

O presente artigo tem por escopo demonstrar que o acesso fácil a dispositivos eletrônicos e, consequentemente, à rede mundial de computadores, tornou a Internet campo fértil para a prática de crimes cibernéticos e instrumento facilitador de condutas ilícitas, as quais, na maioria das vezes, é perpetrada de forma oculta e sem testemunhas.

Verifica-se que o Brasil, não obstante ser um dos países que mais utiliza a Internet, não possui em seu ordenamento jurídico norma específica e unificada que alcance todas as condutas tipificadas penalmente, situação, contudo, que pretende ser solucionada com a recente entrada em vigor no Brasil da Convenção de Budapeste cujo benefício maior é a proteção e segurança aos usuários da Internet, o combate eficaz à anonimização, além do fornecimento de ferramentas forenses, instrumentos processuais de cooperação internacional e a qualificação das autoridades que investigam.

É possível afirmar que atualmente as penas impostas para a punição dos que praticam crimes cibernéticos encontram-se previstas na norma penal e em legislações extravagantes, cuja quantificação ainda é leve e não produz o efeito impeditivo pretendido, ou seja, os criminosos reiteram na conduta, na certeza de que não sofrerão maiores sanções penais.

O conteúdo apresentado trata, principalmente, dos desafios da investigação cibernética desde a coleta e preservação da prova digital até a resistência por parte de determinados provedores de Internet em cumprir integralmente a legislação do Marco Civil, ressaltando, ainda, os mecanismos e sistemas de anonimização, como uso de rede TOR e VPN, passando pelo uso da *Deep Web* e *Dark Web* e de endereços IPs compartilhados, que dificultam, ainda mais, a individualização da conduta criminosa, e consequentemente, a descoberta da autoria do crime.

O tema aqui discorrido é relevante não apenas para o estudo doutrinário, mas, principalmente, para a prática no curso das investigações para identificação da autoria e/ou comprovação da materialidade. Sem o conhecimento das normas penais apresentadas e das peculiaridades inerentes a matéria corre-se o risco da perda da prova digital e do insucesso na empreitada.

Não se pode olvidar, contudo, que mesmo diante de todas as dificuldades existentes e da limitação legislativa sobre o tema, muito se pode fazer para combater os crimes cibernéticos, em especial, diante das previsões legais do Lei do Marco Civil da Internet que determina a aplicação da lei brasileira aos provedores de Internet que prestam seus serviços no território brasileiro, disciplina os prazos de guarda/preservação dos registros de conexão e impõe a obrigação legal de fornecimento de dados cadastrais e pessoais às autoridades brasileiras, cabendo a estas últimas, a dedicação e empenho na atividade investigativa.

A empreitada ganha força com a promulgação da Convenção de Budapeste que desde março de 2023 ingressou no ordenamento jurídico brasileiro trazendo novos instrumentos de cooperação jurídica internacional com a perspectiva de tornar célere, eficiente e eficaz a obtenção de provas digitais quando estas estiverem armazenadas em outros Estados.

Importante frisar que ainda que sejam vários os mecanismos utilizados na busca da prova digital, através de requisição direta ou por meio de ordem judicial, a Lei do Marco Civil da Internet, também conhecida como "CONSTITUIÇÃO DA INTERNET", ratificou expressamente em seu texto legal os princípios e garantias individuais, sobretudo, aqueles que preservam a privacidade e intimidade, sobrepondo-se estes ao dever estatal de investigar, sob pena de nulidade da prova obtida.

REFERÊNCIAS

ARAS, Vladimir. Crimes de informática. Uma nova criminalidade. **Jus Navigandi**, Teresina, ano 5, p. 51, out. 2001. Disponível em: <https://jus.com.br/artigos/2250/crimes-de-informatica>. Acesso em: 28 maio 2024.

ARAS, Vladimir. O Congelamento de dados Informáticos para fins de prova no processo penal. **DELICTAE**, Vol. 8, Nº15, Jul.-Dez. 2023. Disponível em: <https://delictae.com.br/index.php/revista/article/view/225/162>. Acesso em: 28 maio 2024.

BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de Investigação Cibernético à luz do Marco Civil da internet**. Rio de Janeiro: Bransport, 2016.

CASTRO, Carla Rodrigues Araújo de. **Crimes de Informática e seus Aspectos Processuais**. 2. ed. Rio de Janeiro: Lumen Juris, 2003.

CONVENÇÃO SOBRE O CIBERCRIME. Disponível em: <https://www.coe.int/en/web/cybercrime/home>. Acesso em: 28 maio 2024.

FELICIANO, Guilherme Guimarães. Informática e Criminalidade: parte I: Lineamentos e Definições. **Boletim Instituto Manoel Pedro Pimentel**, São Paulo, v. 13, n. 2, 2000.

GRECO FILHO, Vicente. Algumas observações sobre o direito penal e a Internet. **Boletim IBCCrim**. São Paulo. Ed. Esp., ano 8, n. 95, outubro, 2000.

JESUS, Damásio MILAGRE, José Antônio. **Marco Civil da Internet**: comentários à Lei 12.965, de 23 de abril de 2014. São Paulo: Saraiva, 2014.

JORGE, Higor Vinicius; Wendt, EMERSON. **Crimes Cibernético, Ameaças e Procedimentos de investigação**. Rio de Janeiro: Editora Basport, 2012.

MINISTÉRIO PÚBLICO FEDERAL. **Roteiro de Atuação sobre Crimes Cibernéticos**: Brasília: MPF, outubro, 2013.

NIGRI, Deborah Fisch. Crimes e segurança na *Internet*. In **Verbis**, Rio de Janeiro: Instituto dos Magistrados do Brasil, Ano 4, n. 20, 2000.

MURATA, Ana Maria Lumi Kamimura; TORRES, Paulo Ritzmann. A Convenção de Budapeste sobre os crimes cibernéticos foi promulgada, e agora?. **Boletim IBCCrim** – ANO 31, Nº 3638 - julho, 2023.