UNIVERSIDADE DO VALE DO RIO DOS SINOS - UNISINOS
UNIDADE ACADÊMICA DE GRADUAÇÃO
CURSO DE DIREITO

MATHEUS GIBOSKI MOREIRA DA SILVA

A CONVENÇÃO DE BUDAPESTE E A COOPERAÇÃO JURÍDICA INTERNACIONAL COMO FERRAMENTAS ESSENCIAIS NA REPRESSÃO AOS CRIMES CIBERNÉTICOS NO BRASIL

São Leopoldo
2021

MATHEUS GIBOSKI MOREIRA DA SILVA

A CONVENÇÃO DE BUDAPESTE E A COOPERAÇÃO JURÍDICA INTERNACIONAL COMO FERRAMENTAS ESSENCIAIS NA REPRESSÃO AOS CRIMES CIBERNÉTICOS NO BRASIL

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do título de Bacharel em Ciências Jurídicas e Sociais, pelo Curso de Direito da Universidade do Vale do Rio dos Sinos – UNISINOS

Orientador: Prof. Ms. Fábio Motta Lopes

São Leopoldo

2021

A Deus por me dar forças para continuar e me abençoar todos os dias.

Aos meus pais pelo apoio, carinho, dedicação e por serem minha base.

AGRADECIMENTOS

Primeiramente, agradeço a Deus por ter me dado forças e guiado durante toda a graduação. Sem a guarda dele eu não chegaria aqui.

Agradeço infinitamente aos meus pais que não mediram esforços e batalharam muito para me dar a oportunidade de chegar ao Ensino Superior. Durante a elaboração desse trabalho e nos momentos mais angustiantes foram eles que estavam lá para me apoiar e me prestar todo o suporte. Sem eles eu não seria nada.

Agradeço aos meus amigos, os quais não poderia citar todos aqui em virtude de ter sido abençoado por Deus e ter conquistado vários durante toda a minha vida, por entenderem as minhas responsabilidades e compreenderem minha ausência em alguns momentos de celebração.

Em especial, agradeço a minha amiga Laura da Silva Fritsch, também aluna da graduação de Direito, por ter acompanhado de perto minha graduação, realizando diversas disciplinas juntos. Foi minha parceira nas aulas e continua sendo minha parceira na vida.

Agradeço ao meu orientador Fábio Motta Lopes, do qual tenho grande admiração, cujo auxílio, compreensão e paciência durante a trajetória do presente trabalho foram essenciais para a concretização desse sonho.

“Quando a vida jogar pedras, não se deixem abalar. Estou certo de que meu amor pelo que fazia é o que me manteve ativo. É preciso encontrar aquilo que vocês amam - e isso se aplica ao trabalho tanto quanto à vida afetiva. Seu trabalho terá parte importante em sua vida, e a única maneira de sentir satisfação completa é amar o que vocês fazem. Caso ainda não tenham encontrado, continuem procurando. Não se acomodem. Como é comum nos assuntos do coração, quando encontrarem, vocês saberão.”[1]

[1] Steve Jobs ao discursar para uma turma de formandos da Universidade de Stanford, nos Estados Unidos, em 2005.

RESUMO

O avanço tecnológico abre fronteiras antes inexploradas pelos seres humanos. Em especial, o surgimento da internet alterou o modo de vida da sociedade em geral, seja para um lado profissional ou pessoal, criando quase que uma dependência da ferramenta. Formas de trabalho e até mesmo o contato com círculos sociais são apenas exemplos de conveniências e facilidades trazidas com a internet. Entretanto, o uso desse instrumento mundial de propagação instantânea e multitarefas atrai o olhar de pessoas más intencionadas e prontas para obter vantagem sobre um sistema complexo e que, mesmo embora quase todas as pessoas a utilizem, poucas possuem conhecimento técnico para se proteger dessas ameaças. Os crimes cibernéticos são uma realidade extremamente atual e uma preocupação urgente que os Estados devem possuir, inclusive pelo fato de os próprios governos também serem alvos de cibercriminosos. Para tanto, como uma forma de reprimir essas condutas delitivas que não respeitam barreiras fronteiriças, diferentemente dos crimes comuns, países do mundo todo devem adotar medidas e cooperarem entre si, facilitando a troca de informações, a aproximação diplomática e evitando conflitos de soberania, buscando um ambiente cada vez mais seguro aos usuários de internet dentro de seus respectivos países. A Convenção de Budapeste representa o principal marco de cooperação internacional na repressão dos crimes cibernéticos e, infelizmente, o Brasil ainda não aderiu ao tratado, embora a medida seja urgente dentro de um dos países que mais sofre com crimes cibernéticos.

Palavras-chave: Crime cibernético. Convenção de Budapeste. Cooperação Jurídica Internacional.

ABSTRACT

The technological advance opens up frontiers previously unexplored by human beings. In particular, the emergence of the internet has changed the way of life of society in general, whether professional or personal, creating almost a dependency on the tool. Ways of working and even contact with social circles are just examples of conveniences and facilities brought about by the internet. However, the use of this global instrument of instantaneous propagation and multitasking attracts the eyes of malicious people ready to take advantage of a complex system and, even though almost everyone uses it, few have the technical knowledge to protect themselves from these threats. Cybercrime is an extremely current reality and an urgent concern that States must have, inclusive because the governments themselves are also targets of cybercriminals. Therefore, as a way of repressing these criminal conducts that do not respect border barriers, unlike common crimes, countries around the world must adopt measures and cooperate with each other, facilitating the exchange of information, diplomatic rapprochement and avoiding conflicts of sovereignty, seeking an increasingly safe environment for internet users inside their respective countries. The Budapest Convention represents the main framework for international cooperation in the repression of cybercrime and, unfortunately, Brazil has not yet adhered to the treaty, although the measure is urgent in one of the countries that suffer most from cybercrime.

Keywords: Cyber crime. Budapest Convention. International Judicial Cooperation.

SUMÁRIO

1 INTRODUÇÃO

A tecnologia pode ser considerada como uma forma de avanço da humanidade em criação de coisas para simplificar a vida das pessoas. Dentre os maiores avanços, indubitavelmente a internet foi o maior deles, sendo quase impossível pensar em um cotidiano nos dias atuais sem a ferramenta.

No entanto, se por um lado a internet possui um imenso impacto na vida das pessoas em termos de compartilhamento de informações, praticidade dos atos da vida comum e entretenimento, também é verdade que, dada sua magnitude, torna-se um ambiente propício para a pratica de atividades ilícitas, tendo em vista a dificuldade na identificação dos agentes praticantes. O anonimato, o fluxo intenso de usuários, dentre outros aspectos que serão debatidos, dificultam a repressão de crimes pelo meio virtual.

Diante de todo esse parâmetro, a situação se agrava ainda mais pelo fato de o crime cibernético não delimitar sua territorialidade. Pior do que isso, ele não respeita limites fronteiriços dos países e ainda se permite ocorrer em diversos locais simultaneamente.

Para combater essa modalidade, a criação de mecanismos já é realidade em diversos países, mas, infelizmente, ainda pouco difundido e explorado, dada sua complexidade. Além disso, conforme mencionado, a falta de limitação territorial para o cibercrime torna a investigação burocrática, conflitante entre Estados e propensa à impunidade. Assim, a solução que esses países devem encontrar é no mútuo auxílio internacional, na cooperação jurídica e na elaboração de tratados que ajudem a efetiva persecução penal.

A Convenção de Budapeste é o primeiro tratado internacional que trata especificamente dos crimes cibernéticos e representa um marco quanto ao assunto. Por meio dela, países da Europa se comprometeram em adotar diversas medidas que buscam a segurança de usuários na internet, além de cooperarem entre si em investigações e, desde então, diversos países têm aderido ao tratado. No entanto, o Brasil, apesar de convidado, ainda não aderiu à Convenção.

O presente trabalho irá apresentar os motivos da necessidade dessas medidas internacionais acontecerem para que o crime cibernético seja, de fato, reprimido, especialmente no Brasil, um dos maiores países vítima de crimes virtuais. Para isso, será necessário apresentar conceitos básicos da internet para a melhor

compreensão do contexto, bem como uma breve história de seu surgimento; analisar exatamente a forma com que o direito brasileiro vem lidando com as novas práticas de ilícito pelo meio digital e o que o país tem adotado de medidas que visam a segurança online. Mais do que isso, analisar-se-á também como andam ocorrendo as investigações, a coleta de provas e os mecanismos que auxiliam a polícia judiciária na repressão dos chamados crimes cibernéticos; e, por fim, examinar as formas de cooperação internacional que o mundo vem apresentado na repressão do cibercrime, especialmente a Convenção de Budapeste, bem como o papel do Brasil na cooperação jurídica internacional quanto ao tema.

O Direito, como ciência jurídica e social, também avança conforme a humanidade e sempre se contextualiza com o momento histórico em que se vive. Nesse sentido, mostra-se a relevância do estudo desse tema extremamente atual, de forma a auxiliar na evolução do direito, evitando sua defasagem e para que se adeque a uma realidade já vivenciada e que tende a ficar ainda mais digital e complexa com o passar dos anos.

O presente trabalho utiliza métodos analíticos, comparativos e dialéticos para fundamentar e defender a posição do autor quanto ao tema estudado.

2 A EVOLUÇÃO DA INTERNET E O SURGIMENTO DO CIBERCRIME

O surgimento da internet é um marco temporal na história da humanidade. Sua criação também é recente: não faz um século de sua existência. Criada no final dos anos 60, ela surge com uma ideia promissora do governo estadunidense de manter as comunicações internas do país em caso de eventual ataque da União Soviética durante o período da guerra fria[1].

Com o passar dos anos, a internet também começou a ser utilizada por outros serviços como universidades, hospitais, educação, dentre tantos outros. O que antes servia com o único propósito de compartilhar informações entre militares distantes, começa, a partir daí, a formar o mundo digital de compartilhamento mundial de informações em massa que conhecemos hoje. No entanto, apenas em meados da década de 90 a internet por provedores comerciais chegou ao Brasil[2], por meio da Norma 004/95[3], redigida pelo Ministério das Comunicações, regulando o uso de meios de rede pública de telecomunicações para o provimento e a utilização de serviços de conexão à Internet.

É absolutamente inegável a importância da ferramenta. A singularidade, praticidade e agilidade de se fazer coisas através da internet simplificou muito a vida dos que a utilizam. Desde comunicação com parentes distantes a compras sem sair de casa, passando pelo entretenimento, tudo instantâneo, certo é que a internet faz, hoje em dia, ser a sociedade quase que dependente dela.

Apenas no Brasil, segundo o censo do Instituto Brasileiro de Geografia e Estatística (IBGE) de 2018, o país registra mais de 126 milhões de usuários[4]. Isso demonstra que mais da metade da população brasileira está conectada. Ainda, os números dos brasileiros que utilizam a internet com algum serviço online, como compras, serviços de streaming, é de 48%, quase metade dos usuários, segundo

---

[1] BARRETO, Alessandro Gonçalves; KUFA, Karina; SILVA, Marcelo Mesquita. **Cibercrimes e Seus Reflexos no Direito Brasileiro**. Salvador: Editora Juspodivm, 2020.

[2] BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silvera. **Manual de Investigação Cibernética: à Luz do Marco Civil da Internet**. Rio de Janeiro: Editora Brasport, p. 1, 2016.

[3] BRASIL. Agência Nacional de Telecomunicações. **Norma nº 004/95**. Uso de Meios da Rede Pública de Telecomunicações para acesso à Internet. Aprovada pela Portaria nº 148/95. Brasília, DF: ANATEL, [1995]. Disponível em: https://www.anatel.gov.br/hotsites/Direito_Telecomunicacoes/TextoIntegral/ANE/prt/minicom_19950531_148.pdf. Acesso em: 27 abr. 2021.

[4] PESQUISA NACIONAL POR AMOSTRA DE DOMICÍLIOS CONTÍNUA. **Acesso à Internet e à televisão e posse de telefone móvel celular para uso pessoal 2017**. Brasília, DF: PNAD contínua, [2018]. Disponível em: https://biblioteca.ibge.gov.br/visualizacao/livros/liv101631_informativo.pdf. Acesso em: 23 ago. 2020.

pesquisa do Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic)[5].

Como se não fosse suficiente, é de notório conhecimento que serviços públicos dependem da internet para seu funcionamento atualmente, bem como grande parte da economia mundial é movimentada por meio dela. Isso prova que a internet tomou proporções que tornam impossível sua irreversibilidade e, mais do que isso, revelam sua importância e seu crescimento exponencial.

Contudo, apesar de seus avanços e dos benefícios trazidos à sociedade, diante da sua magnitude, a falsa sensação de proteção por trás de uma tela e outros aspectos que serão abordados a frente, a internet também tornou o ambiente digital muito propício ao cometimento de crimes e atos ilegais.

Christina Kunrath[6] refere que

> Passar um período do dia *on-line*, ou seja, conectado com a internet, tornou-se algo necessário na sociedade contemporânea, inexoravelmente adaptada à comunicação instantânea, que diminui as distâncias e incrementa a globalização. Tudo isso aproxima a vida real do mundo cibernético, e parece criar um novo *locus* — o ciberespaço, despertando o interesse da sociedade interconectada, bem como do Direito, face aos perigos e conflitos que surgem com a conectividade.

O fato é que a tecnologia, por apresentar novas ferramentas desconhecidas e complexas de se manusear por grande parte das pessoas ainda, além de quase que impor uma “obrigação” de seu uso, torna aqueles que não possuem conhecimento na área mais propensos a caírem em golpes, enquanto os mais experientes especialistas na prática do ilícito e no seu próprio desaparecimento. Ficou mais fácil, portanto, ao criminoso sair impune pelo seu crime. Segundo Gustavo Têsta Correa, “a internet é um paraíso de Informações, e, pelo fato de essas serem riqueza, inevitavelmente atraem o crime. Onde há riqueza, há crime.”[7]

---

[5] CENTRO REGIONAL DE ESTUDOS PARA O DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO. **TIC Domicílios:** Pesquisa sobre o Uso das Tecnologias de Informação e Comunicação nos Domicílios Brasileiros 2018. São Paulo: Comitê Gestor da Internet no Brasil, 2019. Disponível em: https://cetic.br/media/docs/publicacoes/2/12225320191028-tic_dom_2018_livro_eletronico.pdf. Acesso em: 23 ago. 2020.

[6] KUNRATH, Josefa Cristina Tomaz Martins. **A expansão da criminalidade no ciberespaço:** desafios de uma política criminal de prevenção ao cibercrime. 158 f. il. 2014. Dissertação (Mestrado) — Faculdade de Direito, Universidade Federal da Bahia, Salvador, p. 16, 2014

[7] CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 5. ed. São Paulo: Saraiva, 2010.

Para se ter uma noção, há pesquisas que apontam que, apenas no Brasil, entre fevereiro e abril de 2020, o aumento de ataques cibernéticos a ferramentas que permitem o acesso remota cresceu 333%[8]. Esse número cresceu drasticamente em virtude da pandemia causada pelo novo Coronavírus, que readequou a rotina de várias pessoas que, agora, trabalham pelo *home office*. Nesse tipo de golpe, os criminosos "invadem os sistemas, sequestram dados e deixam a rede interna criptografada", impedindo o serviço. Depois de estar com o controle dos serviços em mãos, eles solicitam resgate para liberar os dados e evitar que os disponibilizem na *deep web*.

Exemplo do ocorrido foi o recente ataque hacker aos sistemas do Tribunal de Justiça do Rio Grande do Sul (TJRS), no final de abril deste ano[9]. Em especial, esse ataque afetou outras instituições importantes e especiais no combate dos crimes cibernéticos, uma vez que o ataque também compromete investigações em andamento, dados sigilosos de operações e até mesmo agentes públicos que estão com dados sob sigilo[10].

Ainda, apenas em 2020, o número de denúncias sobre crimes cibernéticos mais que dobrou em relação ao ano de 2019, somando mais de 156 mil denúncias, segundo dados das notificações recebidas pela Central Nacional de Denúncias de Crimes Cibernéticos, parceria entre a ONG Safernet Brasil e o Ministério Público Federal (MPF)[11]. As principais denúncias foram sobre pornografia infantil, chegando a quase cem mil.

---

[8] OLIVEIRA, Regiane; ROSSI, Marina. No submundo da internet, prospera o lucrativo negócio de chantagear empresas em meio à pandemia. **El País Brasil**, São Paulo, 03 jul. 2020. Disponível em: https://brasil.elpais.com/tecnologia/2020-07-03/no-submundo-da-internet-prospera-o-lucrativo-negocio-de-chantagear-empresas-em-meio-a-pandemia.html. Acesso em: 01 mai. 2021.

[9] ALECRIM, Emerson. Ataque hacker derruba sistemas do TJRS com ransomware: TJRS aparenta ter sido alvo de ransomware do grupo REvil, que teria pedido resgate de US$ 5 milhões. **Tecnoblog**, Brasil, 30 abr. 2021. Disponível em: https://tecnoblog.net/437846/ataque-hacker-derruba-sistemas-tjrs-ransomware/. Acesso em: 01 mai. 2021.

[10] ROSA, Vitor. Investigações estão prejudicadas de maneira quase irreversível, diz chefe do MP sobre ataque hacker ao TJRS: Procurador Fabiano Dallazen se refere aos atrasos que serão gerados em escala e, também, ao temor do vazamento de dados. **GZH,** Porto Alegre, 30 abr. 2021. Disponível em: https://gauchazh.clicrbs.com.br/geral/noticia/2021/04/investigacoes-estao-prejudicadas-de-maneira-quase-irreversivel-diz-chefe-do-mp-sobre-ataque-hacker-ao-tjrs-cko4s4pc400be018mrlsoeq90.html. Acesso em: 01 mai. 2021.

[11] DENÚNCIAS de crimes cometidos pela internet mais que dobram em 2020: Foram 156.692 notificações anônimas de janeiro a dezembro do ano passado, contra 75.428 em 2019. Ocorrências foram lideradas, mais uma vez, pela pornografia infantil, com quase 100 mil acusações. **G1,** Brasil, 09 fev. 2021. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/02/09/numero-de-denuncias-de-crimes-cometidos-pela-internet-mais-que-dobra-em-2020.ghtml. Acesso em: 01 mai. 2021.

Estes são só alguns dos diversos crimes que ocorrem no meio digital e que vem crescendo exponencialmente todos os dias. E não são apenas os crimes que têm como interesse o roubo de dados, pornografia infantil ou invasão de outros dispositivos que ocorrem pelo meio digital. Os crimes comuns, como estelionato e furto, também vem apresentando uma crescente onda de ocorrências[12]. O fato é que, embora a grande conveniência que a internet propõe aos usuários, ao mesmo tempo se está exposto a agentes mal intencionados, e estes, embora a falsa sensação de anonimato por usarem uma ferramenta que possibilita ataques e atitudes ilícitas por meio não-físico, não devem se sentirem intocáveis e invulneráveis à justiça.

Mesmo que já tenha sido realizada convenção para tratar especificamente do assunto, como a Convenção de Budapeste, que será abordada mais à frente, o Brasil não a aderiu ainda, e muito por esse motivo deixa a desejar quanto à segurança cibernética e o combate aos delitos informáticos.

A internet ainda é um local complexo e difícil para a maioria das pessoas. E se nem a sociedade como um todo conseguiu se adaptar inteiramente à era informatizada, o Direito, como regulamentador de condutas, também ficou pra trás, mas já possui uma ideia da amplitude do cibercrime e como ele vem ocorrendo.

2.1 A ATUAÇÃO DE *HACKERS* NA *DEEP WEB*

Os hackers são normalmente associados à criminalidade, mas não necessariamente um hacker é um criminoso. Na verdade, uma pessoa que possua denso conhecimento na tecnologia da informação e tenha habilidade de "modificação" de determinada aplicação eletrônica pode ser considerada hacker. Para se ter uma ideia, não são raros os casos em que empresas oferecem prêmios em dinheiro à hackers para eles encontrarem brechas nos seus sistemas[13]. Esse método tem sido utilizado para que essas companhias consigam explorar erros e

[12] CARONE, Carlos. Estelionato na internet cresceu mais de 1.200% no DF durante pandemia: Metrópoles teve acesso a mapeamento dos crimes em todas as regiões do DF. De fraude a pedofilia, veja os cibercrimes que mais têm aumentado. **Metrópoles,** Brasília, DF, 12 abr. 2021. Disponível em: https://www.metropoles.com/distrito-federal/estelionato-na-internet-cresceu-mais-de-1-200-no-df-durante-pandemia. Acesso em: 01 mai. 2021.

[13] APPLE oferece US$ 1 milhão para quem hackear iPhone: O prêmio será concedido para pesquisadores e engenheiros de sistemas que encontram falhas no núcleo do sistema operacional iOS. **Época Negócios Online**, Rio de Janeiro, 12 de ago. de 2019. Disponível em: https://epocanegocios.globo.com/Empresa/noticia/2019/08/apple-oferece-us-1-milhao-para-quem-hackear-iphone.html. Acesso em: 26 ago. 2020.

falhas de segurança com o intuito de aprimorarem e aperfeiçoarem seus produtos e sistemas. Diferentemente dos *crackers*, estes sim têm a intenção de prejudicar terceiros. Esse é o cibercriminoso que as instituições judiciárias buscam punir.

O acesso a sites de busca, notícias, redes sociais, jogos digitais dentre outros é apenas uma face da internet que se conhece e também a suficiente para suprir a necessidade dos usuários. A melhor forma de se ilustrar o emaranhado de conexão que é a internet seria um iceberg. Imagina-se que na ponta estão os sites anteriormente citados, ou seja, aqueles de uso comum do dia-a-dia de qualquer usuário. Tudo isso é apenas a ponta do iceberg. Abaixo da linha do mar se encontraria a parte obscura da internet e, conforme mais fundo, mais perigoso.

A *deep web (*ou também chamada *dark web)* é exatamente essa parte abaixo da ponta do iceberg. O lugar é repleto de fóruns, páginas e blogs que não podem ser acessados por meio de um buscador comum, como o Google, e possui uma explicação para isso. Nesse espaço, é fácil encontrar uma rede de crimes e criminosos virtuais. Pedófilos, mercenários, exploradores sexuais, terroristas, pirataria e outros cibercriminosos utilizam esse espaço para compartilhar seus serviços, uma vez que o requisito para a navegação dessa área é a utilização de aplicações e programas que mascaram a localização e quase que impossibilitam a identificação do usuário. Em suma, a *deep web* engloba o mercado negro da internet e, por consequência, as transações quanto aos serviços também são camufladas.

Por ser uma área de difícil acesso ao usuário comum da internet, bem como pelo fato de os usufruidores e prestadores dos serviços lá encontrados possuírem meios de garantir seu anonimato e dificultar muito a sua localização, aliado à falta de estrutura dos Estados no monitoramento e repressão dos delitos lá praticados, o local se tornou o principal meio dos criminosos cibernéticos para o cometimento de ilícitos.

2.2 O *CIBERCRIME* E A CLASSIFICAÇÃO DOS CRIMES CIBERNÉTICOS

O prefixo “ciber” é derivado de *cyber*, do diminuitivo de *cybernetic* (cibernético, em inglês) e condiz com tudo relacionado à tecnologia, especialmente aos computadores, no geral[14]. A junção do termo com “crime” condiz com os delitos

[14] SIGNIFICADOS BR. **Significado de Cyber**. Brasil, [20--]. Disponível em: https://www.significadosbr.com.br/cyber. Acesso em: 29 ago. 2020.

cometidos no âmbito tecnológico, precisamente com a utilização de equipamentos computacionais para a sua prática.

No entanto, o uso da terminologia "*cybercrime*", apesar de majoritariamente utilizada, não é pacífico entre os pesquisadores do assunto, uma vez que ela não estaria albergando todos os conceitos de crimes cometidos com o uso de computadores ou tecnologia. Como assevera Alessandro Gonçalves Barreto, Karina Kufa e Marcelo Mesquita Silva, não se trata de mero tecnicismo. Isto é, "a ausência de padronização (...) impede um melhor levantamento estatístico, dificulta a implementação de ações preventivas e repressivas."[15]

A Convenção de Budapeste, realizada em 2001, da qual o Brasil apenas manifestou interesse na adesão ao instrumento internacional[16], reconheceu a necessidade de uma política criminal comum e internacional entre os membros da convenção a respeito dos crimes virtuais e assim definiu o cibercrime[17]:

> Os atos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta de desses sistemas, redes e dados.

Para Augusto Rossini,[18]

> "delito informático" poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade a confidencialidade.

---

[15] BARRETO, Alessandro Gonçalves; KUFA, Karina; SILVA, Marcelo Mesquita. **Cibercrimes e Seus Reflexos no Direito Brasileiro**. Salvador: Editora Juspodivm, 2020.

[16] GOVERNO FEDERAL. Ministério das Relações Exteriores. **Notas à Imprensa nº 309/2019:** Processo de adesão à Convenção de Budapeste - Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública. Brasília, DF: Ministério das Relações Exteriores, 11 dez. 2019. Disponível em: https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/2019/processo-de-adesao-a-convencao-de-budapeste-nota-conjunta-do-ministerio-das-relacoes-exteriores-e-do-ministerio-da-justica-e-seguranca-publica. Acesso em: 29 ago. 2020.

[17] BRASIL. Ministério Público Federal. **Convenção Sobre o Cibercrime.** Budapeste, 23 nov. 2001. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf. Acesso em: 29 ago. 2020.

[18] ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004.

Apesar de ser um conceito relativamente novo, os cibercrimes já possuem suas classificações e conceitos.

Os cibercrimes podem ser classificados de duas formas: os próprios e os impróprios. Nos crimes próprios, sistemas informatizados, redes, bancos de dados, arquivos, dentre outros instrumentos informatizados são o objetivo de ataque do criminoso, que se utilizam também de meios eletrônicos para tanto. Ou seja, o crime perpetrado pelo agente busca dados informatizados e, para acessá-lo, ele utiliza equipamentos eletrônicos para conseguir, sendo esse um elemento intrínseco do crime. O Código Penal[19] brasileiro já pune algumas condutas nesse sentido, como, por exemplo, a invasão de dispositivo informático, previsto no art. 154-A; a inserção de dados falsos em sistema de informações, previsto no art. 313-A, dentre poucos outros.

Nos crimes impróprios, os dispositivos tecnológicos são apenas o meio para a prática de um delito. Dessa forma, o objetivo final do agente é um resultado no mundo real e físico. Conforme Damásio de Jesus e José Antônio Milagre[20],

> Os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço "real", ameaçando ou lesando outros bens, não-computacionais ou diversos da informática.

Nesse sentido, os crimes impróprios não precisam necessariamente de uma definição jurídica para ser enquadrados no tipo penal, podendo ser adequados nos tipos penais já existentes. Exemplo bastante claro seriam os crimes contra a honra, nos quais o agente os pratica via rede social, expondo terceiro. A rede social foi apenas a ferramenta eletrônica utilizada. O intento de macular a honra da vítima não tem relação objetiva com o meio empregado.

Ao diferenciar a classificação dos cibercrimes, Marcelo Xavier de Freitas Crespo[21] diz o seguinte:

---

[19] BRASIL. **Decreto-lei nº 2.848, de 7 de dezembro de 1940.** Código Penal. Brasília, DF: Congresso Nacional [1940]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 29 ago. 2020.

[20] JESUS, Damásio de; MILAGRE, José Antonio. **Manual de Crimes Informáticos**. São Paulo: Saraiva, 2017.

[21] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011.

> Temos que, para se cometer delitos classificados como impróprios, não se verificam grandes diferenças quanto ao modus operandi. Em outras palavras, embora mude o modo pelo qual se pratica a ação delitiva, não se vislumbra a necessidade de conhecimentos técnicos. Já quanto aos ilícitos classificados como próprios, estes sim, dependem de conhecimento específicos de computação.

Apesar da classificação doutrinária, como o Brasil está em vias de aderir à Convenção de Budapeste, importante destacar a classificação dos cibercrimes segundo o tratado internacional. A Convenção separa os crimes cibernéticos por títulos, conforme:

> Título 1 – Infrações contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos;
> Título 2 – Infrações relacionadas com computadores
> Título 3 – Infrações relacionadas com o conteúdo
> Título 4 – Infrações relacionadas com a violação do direito de autor e direitos conexos

Mais à frente irá se falar a respeito do contraste entre a legislação brasileira com os tratados internacionais e o que o Brasil tem feito no tocante à adoção de medidas para repressão dos crimes cibernéticos, observando esses diplomas.

E é por ser uma modalidade criminosa tão “recente” que se faz necessário o estudo aprofundado de suas ações e consequências dentro de uma sociedade conectada pelo meio virtual. A capacidade de um agente criminoso de conseguir consumar seu intento de forma remota, aliada a uma especialidade técnica que o agente possui de conseguir dificultar sua localização e, consequentemente, dificultar sobremaneira a tarefa investigativa, torna o universo digital um meio propício para o cometimento de crimes com a sensação de que a impunidade será a consequência das ações criminosas.

Dessa forma, o crime cibernético é uma espécie de delito tão complexa que permite que a ação do agente possa ocorrer em diferentes Estados e seus resultados em outros. Tanto é verdade que a cooperação entre os países se torna algo imprescindível na investigação dos crimes. Mas, ainda assim, a competência para investigação e processamento desses delitos continua sendo um desafio das autoridades, tendo em vista sua capacidade volátil de troca de locais dos atos executórios e do local de sua consumação.

2.3 A EXTRATERRITORIALIDADE DA LEI PENAL

É princípio básico constante nos ordenamentos jurídicos o da territorialidade. Por ele, os países aplicam suas leis aos crimes cometidos dentro de sua jurisdição territorial, isto é: crime cometido no país se submete às leis do país onde foi praticado. Correlacionado com o princípio da soberania, o princípio da territorialidade no Brasil tem aspecto um pouco diferente, chamando-se também de Princípio da Territorialidade Temperada. Por meio dele, aplica-se a lei brasileira aos crimes cometidos dentro do país, sem prejuízo da aplicação de convenções, tratados e regras de direito internacional. Ou seja, trata-se de uma flexibilização, na qual a lei estrangeira pode ser aplicada dentro do território nacional se assim exigirem tratados e convenções internacionais.

No caso dos crimes cibernéticos, trata-se de uma modalidade criminosa extremamente complexa e, sabendo que eles costumam acontecer à distância, podendo, inclusive, ocorrerem em mais locais simultaneamente, como anteriormente já debatido, dificulta muito quanto à atribuição da sua territorialidade. Nesse sentido, para início de um processo investigatório dentro do Brasil, é essencial verificar se o crime cometido é positivado na lei brasileira e, se for, qual o local da sua consumação.

Diante disso, surge uma questão importante em termos de persecução dos crimes cibernéticos, a qual também é enfrentada por ordenamentos jurídicos de outros Estados: o que se considera local do crime quanto aos crimes cibernéticos?

O Código Penal brasileiro, em seu artigo 6º, traz a teoria da ubiquidade ao ordenamento jurídico do país, que considera o local do crime onde a ação ou omissão foi praticada, mas também o local onde ocorreu o resultado ou onde ele se pretendia. Em outras palavras, aos crimes iniciados no estrangeiro mas com resultado em território nacional e vice-versa, aplica-se a lei nacional.

Já o artigo 7º, trata das hipóteses de extraterritorialidade, nas quais estão dispostas as hipóteses em que a lei brasileira incide nos crimes cometidos no estrangeiro. No inciso I do artigo, que prevê majoritariamente as hipóteses cometidas contra a administração pública, não se encontram óbices para a aplicação da lei brasileira no caso do cometimento de um crime cibernético contra ela. Ou seja, não há condições para se aplicar a lei brasileira nesses casos.

Diferentemente ocorre com os particulares. O inciso II do artigo refere que os crimes praticados no estrangeiro serão sujeitos à lei brasileira se a) o Brasil, por tratado ou convenção, se obrigou a reprimir; b) se for cometido por brasileiro, e; c) se for praticado em aeronaves, embarcações brasileira, mercantes ou de propriedade privada, quando em território estrangeiro não forem julgados. Essas hipóteses são condicionadas ao parágrafo 2º do mesmo artigo, que apresenta requisitos para incidência da lei brasileira, quais sejam: entrar o agente em território nacional, ser o fato punível também no país em que foi praticado, estar o crime incluído entre aqueles pelos quais a lei brasileira autoriza a extradição, não ter sido o agente absolvido no estrangeiro ou não ter lá cumprido a pena e, por último, não ter sido o agente perdoado no estrangeiro ou, por outro motivo, não estar extinta a punibilidade, segundo a lei mais favorável.

Como se vê, o cumprimento desses requisitos torna a aplicabilidade extremamente dificultosa[22]. A uma que o delito cibernético não precisa da presença da pessoa física para seu cometimento dentro do Brasil, por exemplo, podendo ele ser executado no exterior por meio de equipamento eletrônico. A duas que o resultado, consumação e local do crime serão no exterior, sendo aplicada, portanto, a lei exterior, não havendo alcance da lei brasileira. Além disso, se o crime for praticado por estrangeiro contra brasileiro e este último estiver no exterior, o §3º do art. 7º exige a presença de todos os requisitos antes citados. É quase impossível que o agente estrangeiro entre no Brasil, pois será desnecessário para a consumação do seu intento.

Assim, Fábio Bechara e Dímitri Flores[23] explicam que

> O rol de condições de extraterritorialidade exige requisitos praticamente inaplicáveis aos crimes cibernéticos a distância, de interesse brasileiro, especialmente quando praticados contra particulares, pois requer a condição completamente oposta à natureza dos crimes dessa espécie, que é a exigência da aproximação física entre o autor e o local do resultado criminoso, o que se revela como verdadeiro óbice à persecução penal.

[22] BECHARA, Fábio Ramazzini; FLORES, Dímitri Molina. Crimes Cibernéticos: qual é o lugar do crime para fins de aplicação da pena e determinação da competência jurisdicional?. **Revista Direito Mackenzie**, São Paulo, v. 13, n. 2, 2019. Disponível em: http://editorarevistas.mackenzie.br/index.php/rmd/article/view/13357/10572. Acesso em: 17 set. 2020.
[23] Ibid.

Em 2015, o Superior Tribunal de Justiça[24] adotou o entendimento de que o local onde foi subtraído a coisa não pode ser considerado como o local físico do crime, nos casos de transferências bancárias, sendo esse entendimento também aplicado aos demais crimes em que o local do crime seja o ciberespaço. Na decisão, ainda, a Turma decidiu que nos casos de furto mediante fraude cometido por associação de cibercriminosos, realizados por meio da internet, deve-se prevalecer o local onde se encontram estabelecidos os agentes, porque, segundo o entendimento, seria o local onde são planejadas e executadas as ações, mesmo que os valores furtados estejam em lugares diferentes.

Isso porque, segundo a Corte, os locais de onde são subtraídos os valores são diversos, mas o local de onde partem as ordens e os atos criminosos continuam o mesmo. Assim, nesses casos, o lugar onde se está estabelecida a organização criminosa é considerado o local onde será promovida a investigação, a instrução processual e julgamento, observando os princípios da celeridade e efetividade.

Por outro lado, a decisão apresentada do STJ não contempla todas as hipóteses de crimes cometidos no meio virtual, uma vez que nem sempre é possível identificar em um primeiro momento onde estava o agente, sendo necessário, para tanto, o deferimento de ordens judiciais para obtenção de registros e demais ferramentas para identificação do criminoso. Além disso, para que tais ordens judiciais sejam deferidas, é necessário também saber o juízo competente para apreciação do pedido.

Por exemplo, nos casos em que o agente criminoso publica na internet conteúdo ofensivo a outrem, nessas hipóteses, a teoria da ubiquidade deve ser aplicada, sendo considerado como local do crime o da publicação ou onde a vítima tomou conhecimento dela.

Nesse sentido foi o entendimento do STJ[25] no Conflito de Competência (CC) 107.938, no qual, ao julgar caso em que criminosos publicaram ofensas de cunho

---

[24] BRASIL. Superior Tribunal de Justiça. **Conflito de Competência nº 132.346 - RS (2014/0023833-8)**. Decisão Monocrática do Conflito de Competência. Suscitante: Juízo Federal da 11ª Vara da Seção Judiciária do Estado do Rio Grande do Sul. Suscitado: Juízo Federal da 3ª Vara da Seção Judiciária do Estado da Paraíba; Juízo Federal da 4ª Vara da Seção Judiciária do Estado do Rio de Janeiro. Relator: Min. Rogerio Schietti Cruz, 05 de agosto de 2015. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/893093395/conflito-de-competencia-cc-132346-rs-2014-0023833-8/decisao-monocratica-893093455?ref=juris-tabs. Acesso em: 01 mai. 2021.

[25] BRASIL. Superior Tribunal de Justiça. **Conflito de Competência nº 107.938 - RS (2009/0183264-2).** Conflito de Competência. Processual Penal. Racismo praticado através de publicação de mensagens racistas em sítio de relacionamento. Internet. Identificação dos autores. Necessidade. Local do crime. Lugar de onde foram enviados os textos ofensivos. Ausência de dados aptos a provar

racista, mas não sendo possível identifica-los, decidiu-se que, embora a competência, de regra, seja do juízo em que foram enviadas as mensagens, mas considerando que não houve a identificação dos agentes, o juízo que tomou conhecimento primeiro da investigação é competente para o processamento do feito.

Alessandro Gonçalves Barreto e Beatriz Silveira Brasil[26] defendem o uso da Teoria da Ubiquidade quanto aos crimes cibernéticos, referindo que:

> Assim, em se tratando do local de crime virtual uma ficção jurídica, é imprescindível a interpretação da legislação processual pautada na Teoria da Ubiquidade, para se considerar, caso a caso, o lugar do crime onde ocorreu a ação ou o resultado, visando a busca da verdade real e a escorreita aplicação da lei penal.

É claro que o legislador, na elaboração do Código Penal, não poderia prever a ocorrência dos cibercrimes, modalidade recente de prática delituosa e diversa do comum, sequer imaginada na época. Ainda assim, diante das novas tecnologias, o direito tem um papel fundamental de acompanhar os atos e a evolução da sociedade, devendo se adaptar em conformidade. Por isso, dirimir o conflito de competência quanto à persecução criminal dos cibercrimes entre Estados é assunto extremamente atual e se resolve com a adoção de normas de direito internacional, em especial aos tratados e convenções.

O que se percebe também é que, embora o ciberespaço seja um local distinto do mundo físico, que vai além das normas geográficas, o Brasil e outros países ainda continuam insistindo na aplicação de leis territoriais tradicionais para as condutas cometidas nesse ambiente. Nesse sentido, se reconhecida a jurisdição nacional sobre um fato-crime, deve-se analisar o local da infração, que, geralmente, está prevista no art. 70 do Código de Processo Penal[27].

---

a origem das ofensas. Continuidade do procedimento investigatório. Prevenção. Competência daquele Juízo que primeiro conheceu da investigação. Suscitante: Juízo Federal da Vara Criminal e Juizado Especial Adjunto de Novo Hamburgo - SJ/RS. Suscitado: Juízo Federal da 4ª Vara Criminal da Seção Judiciária do Estado do Rio de Janeiro. Relator: Min. Jorge Mussi, 27 de outubro de 2010. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/17358831/conflito-de-competencia-cc-107938-rs-2009-0183264-2/inteiro-teor-17358832?ref=amp. Acesso em: 01 mai. 2021.

[26] BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silvera. **Manual de Investigação Cibernética: à Luz do Marco Civil da Internet**. Rio de Janeiro: Editora Brasport, p. 28, 2016.

[27] Art. 70 do Código de Processo Penal: A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução.
BRASIL. **Decreto-lei nº 2.848, de 7 de dezembro de 1940.** Código Penal. Brasília, DF: Congresso Nacional [1940]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 29 ago. 2020.

Aqui, o legislador adotou a teoria do resultado como regra para estabelecer as regras para determinação do local do crime, mas existem algumas críticas quanto a adoção dessa teoria quanto aos crimes plurilocais, como é o caso dos crimes cibernéticos, tendo em vista que pode haver uma pluralidade de resultados que podem ocorrer em diversos locais, tudo ao mesmo tempo. Por meio dessa teoria, o local da infração é aquele onde se a consumou ou onde se deu o último ato da tentativa.

Como se verá adiante, a maioria dos tipos penais cibernéticos são considerados delitos formais ou de mera conduta. Nesses casos, entende-se, portanto, que os crimes cibernéticos próprios têm como local de infração, em regra, o mesmo local onde se encontra o dispositivo informático usado para prática do crime. No entanto, quanto aos crimes cibernéticos impróprios, pelos quais o dispositivo informático é usado como meio, espera-se que o local de infração seja diferente de onde se encontra o dispositivo informático, tendo em vista que o resultado se deu em outro local[28].

Assim, o problema surge quanto aos crimes cibernéticos praticados à distância e com multilocais como resultado, sejam eles próprios ou impróprios. Nesse diapasão, os resultados do crime podem ocorrer dentro do território nacional, da mesma forma que podem ocorrer no estrangeiro, simultaneamente. Assim, surgem diversos juízos competentes para processar e julgar o caso, inclusive de jurisdições internacionais.

Na lição de Fábio Bechara e Molina Flores[29]

> Caso a conduta seja praticada em território nacional e o resultado se dê exclusivamente no exterior, o Estado brasileiro reservar-se-á o direito de punir a referida conduta (art. 6º do Código Penal) e terá por juiz natural o magistrado brasileiro com jurisdição sobre o território em que se localizava o dispositivo informático utilizado na infração penal (art. 70, § 1º, do Código de Processo Penal).
> Se houver resultado correspondente a uma ou mais vítimas no interior do território nacional, haverá multiplicidade de juízes competentes, já que haverá configuração de um ou mais resultados em diferentes territórios internos e mais o juiz competente para o resultado externo, sendo cada um deles igualmente competente.

[28] BECHARA, Fábio Ramazzini; FLORES, Dímitri Molina. Crimes Cibernéticos: qual é o lugar do crime para fins de aplicação da pena e determinação da competência jurisdicional?. **Revista Direito Mackenzie**, São Paulo, v. 13, n. 2, 2019. Disponível em: http://editorarevistas.mackenzie.br/index.php/rmd/article/view/13357/10572. Acesso em: 17 set. 2020.
[29] Ibid.

> Nesse caso, os critérios especiais do art. 69, inciso II e seguintes, do Código de Processo Penal deverão ser aplicados para realizar esse "desempate" entre os diversos órgãos judiciários concorrentes.

Entretanto, ainda há a possibilidade do interesse do Estado estrangeiro na persecução penal da conduta praticada no Brasil e que teve resultado no território do estrangeiro. Nessa hipótese, além do conflito de competência internamente, haverá a concorrência entre a jurisdição brasileira e a estrangeira, sendo que cada Estado possui soberania e autonomia para se declarar competente para processamento e julgamento do caso.

No entanto, esse conflito encontra uma solução parcial na Convenção de Budapeste, da qual se falará mais à frente e que o Brasil ainda não é signatário. Na Seção 3, que fala da competência, o artigo 22 da Convenção

> adota o princípio da territorialidade como base legitimadora para que cada Estado puna as condutas cometidas em seu território e determina que o Estado abdique do princípio da nacionalidade, segundo o qual o Estado poderá punir o seu nacional que praticar crime no exterior, em favor do Estado em que houver sido cometido o crime.[30]

Em outras palavras, o Estado em que a vítima sofreu a ação criminosa é competente para processar e julgar o estrangeiro criminoso, sendo que o Estado onde o estrangeiro criminoso é nacional abdica da possibilidade de processar e julgá-lo, em virtude do princípio da nacionalidade, em favor do Estado da vítima.

A Convenção também determina que nas hipóteses em que um Estado estrangeiro capture o criminoso, deve processá-lo ou extraditá-lo, seguindo as possibilidades do seu regimento interno. Por fim, quanto à competência, a Convenção ainda refere a possibilidade dos Estados, onde ocorreram o resultado das ações do crime cibernético, de realizar uma consulta entre si para determinar qual jurisdição prevalecerá, evitando trabalho redobrado, o *bis in idem* e tornando a persecução penal mais ágil, de acordo com o 5º parágrafo do artigo 22, da Seção 3, da Convenção de Budapeste, que diz:

---

[30] BECHARA, Fábio Ramazzini; FLORES, Dímitri Molina. Crimes Cibernéticos: qual é o lugar do crime para fins de aplicação da pena e determinação da competência jurisdicional?. **Revista Direito Mackenzie**, São Paulo, v. 13, n. 2, 2019. Disponível em: http://editorarevistas.mackenzie.br/index.php/rmd/article/view/13357/10572. Acesso em: 17 set. 2020.

> Quando mais que uma Parte reivindique a competência em relação uma presumível infracção prevista na presente Convenção, as Partes em causa, se for oportuno, consultar-se-ão a fim de determinarem qual é a jurisdição mais apropriada para o procedimento penal.[31]

Assim, quanto à extraterritorialidade internacional dos crimes cibernéticos, a concorrência entre Estados dificulta sobremaneira a persecução penal dos crimes cibernéticos. Segundo Fábio Ramazzini Bechara e Dímitri Molina Flores[32]

> conflitos entre as diferentes jurisdições nacionais não possuem, nem poderiam possuir, solução no direito doméstico, mas em normas de direito internacional expressas por meio de tratados, convenções, acordos bilaterais, entre outros.

No tocante à competência interna, o Supremo Tribunal Federal[33] já possui decisão que fixou a tese a respeito da competência jurisdicional para processamento e julgamento dos crimes cometidos pela rede mundial de computadores. Segundo o entendimento, pacificado pela decisão do Recurso Extraordinário 628.624 sobre o art. 241-A do Estatuto da Criança e do Adolescente, que diz respeito ao crime de divulgação e publicação de pornografia infantil, se o conteúdo puder ser acessado no estrangeiro ou há amplo acesso em qualquer parte do mundo, a competência para processamento e julgamento dos crimes será da Justiça Federal.

No caso, a publicação de material pedófilo, quando é feita em sites de amplo e fácil acesso por qualquer pessoa, inclusive de qualquer lugar do globo, por meio da internet, além da intenção do agente de alcançar o maior número possível de pessoas, assumindo, assim, a possibilidade de que pessoas no estrangeiro possam acessar o conteúdo, trazem a característica de internacionalidade do crime. Ainda assim, é prescindível que o material tenha sido acessado efetivamente por um

---

[31] BRASIL. Ministério Público Federal. **Convenção Sobre o Cibercrime.** Budapeste, 23 nov. 2001. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf. Acesso em: 29 ago. 2020.

[32] Ibid.

[33] BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 628.624/MG.** Recurso Extraordinário. Repercussão Geral Reconhecida. Penal. Processo Penal. Crime previsto no artigo 241ª da Lei 8.069/90 (Estatuto da Criança e do Adolescente). Competência. Divulgação e publicação de imagens com conteúdo pornográfico envolvendo criança ou adolescente. Convenção sobre direitos da criança. Delito cometido por meio da rede mundial de computadores (Internet). Internacionalidade. Artigo 109, V, da Constituição Federal. Competência da Justiça Federal reconhecida. Recurso Desprovido. Recorrente: Fábio. Recorrido: Ministério Público Federal. Relator: Min. Marco Aurélio, 29 de outubro de 2015. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=10667081. Acesso em: 01 mai. 2021

estrangeiro para a configuração da competência federal, mas tão somente que o material pudesse ter sido acessado por ele. Portanto, quanto aos crimes previstos nos artigos 241, 241-A e 241-B do Estatuto da Criança e do Adolescente, estes serão processados e julgados pela Justiça Federal, quando praticados por meio da rede mundial de computadores.

Por enquanto, conforme demonstrado, são as decisões jurisprudências que têm norteado o caminho para a definição da competência dentro do território brasileiro.

3 OS DESAFIOS DA INVESTIGAÇÃO E REPRESSÃO AOS CRIMES CIBERNÉTICOS

Feitas as premissas necessárias nos tópicos anteriores para a melhor compreensão do contexto e conceitos do cibercrime, ver-se-ão agora os desafios na investigação e na repressão dos crimes cibernéticos. Conforme amplamente mencionado anteriormente, a internet é um local formado por vários locais, podendo, inclusive, serem internacionais. Além disso, esses locais são cheios de pessoas, ou seja, os usuários.

Qualquer autoridade ao investigar um crime que tenha ocorrido em um lugar de grande aglomeração terá, em determinados casos, grande dificuldade de encontrar o autor, tendo em vista a quantidade de pessoas. É mais ou menos como ocorre na internet. Milhões de usuários simultaneamente, não presenciais de forma física e muitos de forma anônima. A complexidade na investigação dos crimes ocorridos por esse meio denota uma quantidade considerável de agentes que, além disso, devem possuir especialização no âmbito da tecnologia da informação.

Marc Goodman[34] refere que

> Um *hacker* esperto nunca iniciaria de seu apartamento na França um ataque direto contra um banco do Brasil. Em vez disso, rotearia seu ataque de uma rede vulnerável para outra, da França para a Turquia e Arábia Saudita em direção ao seu destino final. Essa capacidade de saltar entre países, uma das maiores forças da internet, cria enormes problemas jurisdicionais e administrativos para a polícia, e é uma das principais razões pelas quais a investigação de crimes virtuais é tão desafiadora e, muitas vezes, inútil.

No entanto, como qualquer outro crime, os cibernéticos não devem ficar impunes por dificuldades na investigação. Em verdade, por se tratarem de modalidade nova e tecnológica e exigido um conhecimento específico para elucidar os delitos, o Direito deve se adequar às novas realidades e trazer formas contundentes de repressão nesses casos, o que já vem sendo feito, mesmo que a passos lentos.

É claro que o Brasil também já se atentou à necessidade de repressão dos crimes cibernéticos. Existem algumas unidades policiais especializadas no combate

---

[34] GOODMAN, Marc. **Future Crimes:** tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso. Rio de Janeiro: Editora Alta Books, p. 16, 2018.

a essa modalidade criminosa, como a Delegacia de Repressão aos Crimes Informáticos (DRCI), no Rio Grande do Sul. No entanto, como amplamente referido, a tecnologia e a internet vieram para ficar. Dificilmente será possível imaginar um mundo sem ela novamente. Apenas no Distrito Federal, entre janeiro e junho de 2020, o número de ocorrências por estelionatos cometidos por meio digital aumentou em 347%, em comparação ao mesmo período do ano passado[35]. Apesar dos números terem grande influência pela pandemia que assola o mundo, isso demonstra um crescimento exponencial de criminalidade virtual. É preciso repensar na ideia de que poucas unidades policiais especializadas na repressão dos crimes digitais sejam suficientes para seu combate.

Ainda, não se quer aqui passar a ideia de que a criação de outras unidades especializadas sejam suficientes e necessárias para a repressão dos crimes cibernéticos. O ideal seria a adoção de políticas criminais para a instrução e treinamento de agentes de delegacias não-especializadas para que tenham capacidade de investigarem o delito. As equipes especializadas, por sua vez, devem prestar o apoio tecnológico e material na coleta de provas e análise dos dados sobre os crimes que a delegacia comum investiga. Conforme pontuam Cerqueira e Rocha[36],

> Toda delegacia de polícia, seja ela especializada ou não, possui o expertise da investigação das condutas descritas pela legislação como crimes, apresenta a estrutura necessária para o ciclo de polícia judiciária e o conhece bem, sendo inerente à sua natureza a investigação preliminar de notícia de crime, a instauração do pertinente inquérito policial, se confirmada a notícia, e o respectivo relatório, ao final. A equipe especializada em crimes cibernéticos participa dos trabalhos com a prestação de apoio, materializado pela realização de procedimentos afetos à tecnologia, entregando à investigação tradicional o conhecimento produzido sobre o crime que a delegacia investiga, subsidiando seus procedimentos de coleta de

[35] BOTELHO, Flávio. Não caia no golpe! Crimes cibernéticos aumentaram 347%: Governo lança cartilhas para te ajudar a evitar armadilhas no mundo virtual. **Agência Brasília**, Brasília, DF, 18 ago. 2020. Disponível em**:** https://agenciabrasilia.df.gov.br/2020/08/17/nao-caia-no-golpe-crimes-ciberneticos-aumentaram-347/#:~:text=Entre%20janeiro%20e%20junho%20deste,mesmo%20per%C3%ADodo%20do%20ano%20passado.&text=Os%20meses%20de%20abril%20e,%3A%20624%20e%20708%2C%20respectivamente. Acesso em: 17 set. 2020.

[36] CERQUEIRA, Silvio Casto. ROCHA, Claudionor. Crimes Cibernéticos: desafios da investigação. **Cadernos ASLEGIS,** Brasília, DF, n. 49, p. 154, mai./ago. 2013. Disponível em: https://www.google.com/url?q=https://www.aslegis.org.br/todas-as-edicoes-artigos/655-cadernos-aslegis-49&sa=D&source=editors&ust=1623087800217000&usg=AOvVaw1NF1RgsfdQyoj2HvmbltSh. Acesso em: 29 ago. 2020.

> prova de materialidade e indícios de autoria sempre que tal se fizer necessário.

Barreto[37] também compartilha do mesmo entendimento:

> Não obstante a criação de delegacias especializadas contribuírem, de forma significativa, na resolução de fatos de difícil elucidação, como homicídios ou ataques a instituições financeiras, a seara dos crimes informáticos é bastante distinta, não dependendo, pois, de apenas um setor com expertise, e sim da polícia como um todo, com capacidade de buscar e materializar a evidência eletrônica.

Além disso, não se pode deixar de destacar o alto custo no treinamento e preparação de autoridades para a investigação do crime cibernético. Essa falta de recursos públicos pode ser suprida com a adoção de parcerias público-privadas com empresas de tecnologia, pois são elas que possuem suporte necessário, aparato tecnológico e humano para ajudar na repressão desses crimes[38].

Como se não fosse o bastante, a polícia judiciária encontra outro desafio constante nas investigações. Segundo a lição de Barreto, Kufa e Mesquita Silva[39], "a atribuição de autoria no ciberespaço depende dos dados fornecidos pelas aplicações de internet". Ou seja, as aplicações de internet são, em sua maioria, de entes privados. Para conseguir dados dessas empresas é necessária a autorização judicial.

O que se tem percebido nas investigações é que muitos desses provedores e aplicações têm se recusado a fornecer dados, especialmente os estrangeiros, que, apesar de possuírem sedes no Brasil, seus bancos de dados e provedores se encontram fora do país. Para esses casos, as empresas do exterior vêm solicitando, para cumprimento das ordens, que sejam elas requeridas através da cooperação jurídica internacional. A principal barreira dessa exigência é o lapso temporal e a burocracia envolvida para o cumprimento. No entanto, não é por esse motivo que a

---

[37] BARRETO, Alesandro Gonçalves. **Análise da lei Azeredo:** necessidade de criação de delegacias e setores especializados na repreensão aos crimes informáticos. Brasil: Migalhas, 11 abr. 2018. Disponível em: https://migalhas.uol.com.br/depeso/278027/analise-da-lei-azeredo-necessidade-de-criacao-de-delegacias-e-setores-especializados-na-repreensao-aos-crimes-informaticos. Acesso em: 09 nov. 2020.

[38] BARRETO, Alessandro Gonçalves; KUFA, Karina; SILVA, Marcelo Mesquita. **Cibercrimes e Seus Reflexos no Direito Brasileiro**. Salvador: Editora Juspodivm, p. 72, p.100, 2020.

[39] Ibid., p. 207.

investigação deva ficar à deriva. Sobre o assunto, Barreto e Caselli e Gaudencio[40] referem:

> A jurisprudência pátria tem reiterado decisões nesse sentido, preconizando que a investigação é pautada pelos princípios da oportunidade e celeridade. Ao adotar a via da assistência mútua internacional, em que pese o esforço do governo brasileiro ao tentar encurtar o tempo de resposta via cooperação, o lapso dilatado para que a polícia acessasse esses dados tornaria, na maioria dos casos, inúteis as informações extemporâneas transmitidas.
> As empresas não podem se negar a prestar informações sob o pretexto de que não possuem acesso a conteúdo armazenado em outro país. Não há como condicionar o cumprimento de uma decisão judicial à localização do servidor, sob pena do Brasil se tornar um paraíso cibernético, onde os entes abstratos aqui se instalam e só arcam com bônus. A persistir um cenário desses, as aplicações de internet irão situar seus servidores em locais em que não haja nenhum tratado de cooperação para furtar-se à aplicação da lei. O local físico do servidor da empresa não pode ser regra de delimitação de competência.

A Lei nº 12.965/2015, conhecida como Marco Civil da Internet, estabelece princípios, garantias e deveres para o uso da internet no território brasileiro e positivou sanções cabíveis aos que descumprem as ordens judiciais. O artigo 12 prevê, além das sanções criminais, cíveis e administrativas aos provedores e aplicações de internet que não respeitarem as ordens judiciais e a proteção aos registros, dados pessoais e comunicação privada, as seguintes penas:

> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;
> III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou
> IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.

[40] CASELLI. Guilherme, BARRETO. Alessandro Gonçalves, GAUDENCIO, Andressa. Aplicação de modernas técnicas de investigação digital pela Polícia Judiciária e sua efetividade. **Direito & TI**, Brasil, 01 mai. 2016. Disponível em: http://direitoeti.com.br/artigos/aplicacao-de-modernas-tecnicas-de-investigacao-digital-pela-policia-judiciaria-e-sua-efetividade**/**. Acesso em: 16 set. 2020.

Recentemente, com a promulgação da Lei nº 13.709/2018[41], conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), surgiu um regulamento de tratamento de dados pessoais que empresas públicas e privadas, que incluem informações de clientes em seus bancos de dados, devem seguir.

A nova legislação vale para todas as empresas que coletem dados pessoais de bens e serviços ofertados a brasileiros, mesmo que operadas de outros países. Assim, a lei acrescentou detalhes importantes para a coleta de dados dentro do território brasileiro e obrigou as empresas estrangeiras que oferecem serviços no Brasil a cumprirem a lei nacional. Inclusive, a jurisprudência pátria também sedimentou o entendimento quanto o assunto:

> EMENTA RECURSO ESPECIAL. INTERNET. JURISDIÇÃO. SOBERANIA DIGITAL. PREQUESTIONAMENTO. AUSÊNCIA. MARCO CIVIL DA INTERNET. ALCANCE. APLICAÇÃO DA LEGISLAÇÃO BRASILEIRA. PERTINÊNCIA DA JURISDIÇÃO NACIONAL. 1. Agravo de instrumento interposto em 29/08/2016, recurso especial interposto em 11/01/2017 e atribuído a este gabinete em 02/05/2018. 2. O propósito recursal consiste em determinar a competência da Poder Judiciário Brasileiro para a determinação do fornecimento de registros de acesso de endereço de e-mail, localizado em nome de domínio genérico ".com". 3. Em conflitos transfronteiriços na internet, a autoridade responsável deve atuar de forma prudente, cautelosa e autorrestritiva, reconhecendo que a territorialidade da jurisdição permanece sendo a regra, cuja exceção somente pode ser admitida quando atendidos, cumulativamente, os seguintes critérios: (i) fortes razões jurídicas de mérito, baseadas no direito local e internacional; (ii) proporcionalidade entre a medida e o fim almejado; e (iii) observância dos procedimentos previstos nas leis locais e internacionais. 4. Quando a alegada atividade ilícita tiver sido praticada pela internet, independentemente de foro previsto no contrato de prestação de serviço, **ainda que no exterior, é competente a autoridade judiciária brasileira caso acionada para dirimir o conflito, pois aqui tem domicílio a autora e é o local onde houve acesso ao sítio eletrônico onde a informação foi veiculada, interpretando-se como ato praticado no Brasil.** Precedente. 5. **É um equívoco imaginar que qualquer aplicação hospedada fora do Brasil não possa ser alcançada pela jurisdição nacional ou que as leis brasileiras não sejam aplicáveis às suas atividades.** 6. Tem-se a aplicação da lei brasileira sempre que 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 ocorra em território nacional, mesmo que

[41] BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais e altera a lei nº 12965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Congresso Nacional [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 08 nov. 2020.

> apenas um dos dispositivos da comunicação esteja no Brasil e mesmo que as atividades sejam feitas por empresa com sede no estrangeiro. 7. Recurso especial parcialmente conhecido e, nessa parte, desprovido.[42] (Grifou-se)

Além disso, o Estado pode, ainda, obter esses dados por motivos de segurança pública, defesa nacional e investigação e repressão de crimes.

A criação da LGPD e do Marco Civil da Internet demonstram, sem dúvidas, um avanço do Brasil ao reafirmar a soberania nacional e seu comprometimento com a defesa nacional, abrindo um meio de desburocratização às exigências feitas por empresas estrangeiras e que atuavam no país. Não obstante, a legislação reforça o combate aos crimes digitais, evitando que o Brasil venha a ser taxado de paraíso do criminoso cibernético.

No entanto, se por um lado as legislações promulgadas até agora a respeito do tema atual tenham estabelecido diretrizes básicas quanto ao uso da internet no Brasil e observações que devem ser atendidas por empresas que utilizam de dados de usuários, ainda assim, a parte técnica e prática de combate e repressão ao crime cibernético deixa a desejar.

3.1 A PRESERVAÇÃO DAS PROVAS NO MEIO DIGITAL

Assim como no mundo real, o crime cometido no meio digital também deixa rastros. No entanto, por ser um ambiente volátil, é muito mais fácil as provas lá serem apagadas ou até mesmo adulteradas. Para evitar que isso aconteça, a investigação criminal possui alguns métodos de obtenção de provas e preservação de evidências.

3.1.1 A VALIDADE DO PRINTSCREEN

Muitos acreditam que a simples captura de tela (chamada de *printscreen*) de alguma aplicação de internet serve como evidência no processo judicial. Entretanto,

---

[42] BRASIL. Superior Tribunal de Justiça (3. Turma). **Recurso Especial Nº 1.745.657 – SP (2018/0062504-5)**. Recurso Especial. Internet. Jurisdição. Soberania Digital. Prequestionamento. Ausência. Marco Civil da Internet. Alcance. Aplicação da Legislação Brasileira. Pertinência da Jurisdição Nacional. Recorrente: Microsoft Informática LTDA. Recorrido: Luis Agostinho Marques Caso Quintiliano; Tam Linhas Aéreas S/A. Relatora: Min. Nancy Andrighi, 03 de novembro de 2020. Disponível em: https://arquivos-trilhante-sp.s3.sa-east-1.amazonaws.com/documentos/informativos-julgados/ffc43ebc9da5bdb81c0b518e9ba925f1.pdf. Acesso em: 01 mai. 2021.

a imagem feita pelo comando do *printscreen* apenas captura o que se está na tela, sem salvar os chamados metadados, que são, basicamente, como se mostra os itens que compõem a página da internet, como, por exemplo, a localização geográfica. Aliado a isso, soma-se o fato de que a captura de tela nada mais é do que uma imagem, podendo ser ela adulterada.

A falta de uma robustez e certeza já tornou esse meio de prova uma discussão em tribunais que entenderam a fragilidade da evidência[43,44].

Nesse sentido, Barreto e Silveira Brasil aduzem que, para que as capturas de tela passem confiabilidade, "é necessário que sejam coletados e conferidos por quem detenha fé pública – nesse caso, escrivão de polícia ou outro servidor que, por meio de lei própria, tenha esse atributo, ou (...), por meio de ata notarial (...)".

O entendimento dos doutrinadores tem base legal no novo Código de Processo Civil (CPC), que prevê em seus artigos 439, 440 e 441:

> Art. 439. A utilização de documentos eletrônicos no processo convencional dependerá de sua conversão à forma impressa e da verificação de sua autenticidade, na forma da lei.
> Art. 440. O juiz apreciará o valor probante do documento eletrônico não convertido, assegurado às partes o acesso ao seu teor.

---

[43] DISTRITO FEDERAL. Tribunal de Justiça do Distrito Federal e Territórios (5. Turma). **Acórdão nº 1019661.** Apelação Cível. Processo 20150110697772APC. [...] 5 - O print screen das telas do sistema da ré não é apto a comprovar a legitimidade das faturas, haja vista ser documento produzido unilateralmente, cujos dados foram inseridos pelos prepostos da ré sem qualquer possibilidade do consumidor ter conhecimento deles [...]. Relatora: Maria Ivatônia, 24 de maio de 2017. Disponível em: https://pesquisajuris.tjdft.jus.br/IndexadorAcordaos-web/sistj?visaoId=tjdf.sistj.acordaoeletronico.buscaindexada.apresentacao.VisaoBuscaAcordao&nomeDaPagina=buscaLivre2&buscaPorQuery=1&baseSelecionada=BASE_ACORDAOS&filtroAcordaosPublicos=false&camposSelecionados=[ESPELHO]&argumentoDePesquisa=&numero=1019661&tipoDeRelator=TODOS&dataFim=&indexacao=&ramoJuridico=&baseDados=[TURMAS_RECURSAIS,%20BASE_ACORDAOS_IDR,%20BASE_TEMAS,%20BASE_ACORDAOS,%20BASE_INFORMATIVOS]&tipoDeNumero=NumAcordao&tipoDeData=DataPublicacao&ementa=&filtroSegredoDeJustica=false&desembargador=&dataInicio=&legislacao=&orgaoJulgador=&numeroDaPaginaAtual=1&quantidadeDeRegistros=20&totalHits=1. Acesso em: 01 mai. 2021.

[44] DISTRITO FEDERAL. Tribunal de Justiça do Distrito Federal e Territórios (1. Turma). **Acórdão nº 824.525**, Apelação Cível do Juizado Especial. Processo nº 20130111169797ACJ. [...] A mera juntada da foto da tela do computador (print screen), cuja informação é produzida unilateralmente e sem o crivo do contraditório e da ampla defesa, não atende os ditames da lei processual, de modo a amparar qualquer juízo de valor negativo à pretensão do autor [...]. Relator: Juiz Luís Gustavo B. De Oliveira, 23 de setembro de 2014. Disponível em: https://pesquisajuris.tjdft.jus.br/IndexadorAcordaos-web/sistj?visaoId=tjdf.sistj.acordaoeletronico.buscaindexada.apresentacao.VisaoBuscaAcordao&nomeDaPagina=buscaLivre2&buscaPorQuery=1&baseSelecionada=TURMAS_RECURSAIS&filtroAcordaosPublicos=false&camposSelecionados=[ESPELHO]&argumentoDePesquisa=&numero=824525&tipoDeRelator=TODOS&dataFim=&indexacao=&ramoJuridico=&baseDados=[TURMAS_RECURSAIS,%20BASE_ACORDAOS_IDR,%20BASE_TEMAS,%20BASE_ACORDAOS,%20BASE_INFORMATIVOS]&tipoDeNumero=NumAcordao&tipoDeData=DataPublicacao&ementa=&filtroSegredoDeJustica=false&desembargador=&dataInicio=&legislacao=&orgaoJulgador=&numeroDaPaginaAtual=1&quantidadeDeRegistros=20&totalHits=1. Acesso em: 01 mai. 2021.

> Art. 441. Serão admitidos documentos eletrônicos produzidos e conservados com a observância da legislação específica.

Especificamente quanto ao uso de fotografias eletrônicas, os artigos 422, §1º e 3º, e 423, também do CPC, discorrem que:

> Art. 422. Qualquer reprodução mecânica, como a fotográfica, a cinematográfica, a fonográfica ou de outra espécie, tem aptidão para fazer prova dos fatos ou das coisas representadas, se a sua conformidade com o documento original não for impugnada por aquele contra quem foi produzida.
> § 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.
> § 3º Aplica-se o disposto neste artigo à forma impressa de mensagem eletrônica.
> Art. 423. As reproduções dos documentos particulares, fotográficas ou obtidas por outros processos de repetição, valem como certidões sempre que o escrivão ou o chefe de secretaria certificar sua conformidade com o original.

Percebe-se, portanto, que a simples imagem da tela não serve como evidência em processo judicial, sendo necessária a adoção de outras medidas para sua validade.

3.1.2 A ATA NOTARIAL E A CERTIDÃO DO ESCRIVÃO

Como visto anteriormente, a ata notarial e a certidão do escrivão são os meios utilizados pela polícia judiciária para conferirem confiabilidade nas provas produzidas. Pela ata notarial, um tabelião, a requerimento da parte interessada, lavra o documento, ficando adstrito à narração dos fatos que presenciou, com indicação do local e dados sobre conteúdo apresentado. Já pela certidão do escrivão, tanto judicial, quanto o de polícia, tem-se a presunção de veracidade no documento confeccionado, fato já pacificado na jurisprudência[45,46]:

---

[45] BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 778.054.** Agravo. Recorrente: Cooperativa Regional dos Produtores de Açúcar e Álcool de Alagoas. Recorrido: Banco Econômico SA. Relatora: Min. Cármen Lúcia, 23 de outubro de 2013. Disponível em: http://www.stf.jus.br/portal/processo/verProcessoPeca.asp?id=181471055&tipoApp=.pdf. Acesso em: 01 mai. 2021.

[46] BRASIL. Superior Tribunal de Justiçal (5. Turma). **Recurso em Habeas Corpus nº 95.784 - PR**. Recurso Ordinário de Habeas Corpus. Tráfico e associação para o tráfico de entorpecentes e porte ilegal de arma de fogo de uso permitido. Negativa de autoria e inexistência de prova de materialidade [...]. Recorrente: Priscila Santos de Castro (preso). Recorrido: Ministério Público do Estado do Paraná.

> (...) RECURSO ESPECIAL. CERTIDÃO RETIFICADA PELO ESCRIVÃO COM BASE EM NOTAS CARTORARAIS. FÉ PÚBLICA. PRESUNÇÃO DE VERACIDADE. (...) 2. As certidões emanadas dos escrivães do Juízo, em razão de seu ofício, revestem-se de presunção juris tantum de legitimidade e de veracidade, em razão da fé pública de que gozam tais agentes auxiliares do juízo. (...) 4. A merda alegação deduzida nas razoes recursais, sem a apresentação de qualquer comprovação que informe as informações certificadas, não pode prevalecer sobre a presunção de legitimidade e de veracidade que gozam as certidões emanadas dos escrivães do Juízo (...)
>
> RECURSO ORDINÁRIO EM HABEAS CORPUS (...) INSUFICIÊNCIA. AUTOS DO INQUÉRITO POLICIAL NÃO-ASSINADAS PELO DELEGADO DE POLÍCIA. IRRELEVÂNCIA. PEÇA MERAMENTE INFORMATIVA. EVENTUAL NULIDADE NO CURSO DO INQUÉRITO POLICIAL NÃO CONTAMINA A AÇÃO PENAL (...) 7. O fato de que as peças dos autos do inquérito policial não possuem a assinatura do delegado de polícia não implica a nulidade do processo, uma vez que o inquérito policial é peça meramente informativa, instrutória, ainda mais porquanto os referidos atos foram rubricados pelo escrivão de polícia, o qual, como investido de forma regular no cargo, possui fé pública e pode conferir veracidade aos documentos.

A ata notarial acaba por não ser frequentemente utilizada no processo criminal, em razão dos custos de sua lavratura. Mas sua previsão está disciplinada no artigo 384 do Código de Processo Civil e os fatos detalhados no documento também são presumidamente verídicos, eis que é documento público e rubricado por tabelião. O artigo 405 do mesmo diploma legal também refere que o documento público faz prova não só da sua formação, mas também dos fatos que o escrivão, o chefe de secretaria, o tabelião ou o servidor declarar que ocorreram em sua presença. Nas duas formas, por óbvio, devem ser precedidos de demais documentos que confirmam a prova, como o próprio *printscreen*, vídeos, dentre outros.

Observa-se que ambos os meios, embora aptos para dar credibilidade aos fatos narrados, ainda parecem ultrapassados e morosos para garantir a eficácia da validade das provas.

Relator: Min. Joel Ilan Paciornik, 06 de dezembro de 2018. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1780840&num_registro=201800552717&data=20181219&peticao_numero=-1&formato=PDF. Acesso em: 01 mai. 2021.

Para isso, já existem *softwares* desenvolvidos que permitem salvar uma página inteira da internet com os metadados necessários, como, por exemplo, o HTTrack[47], que possibilita o download de páginas da internet com todos os fragmentos de dados. O programa é grátis e faria grande diferença na investigação policial. Seria interessante o desenvolvimento de softwares pelo Poder Público que também auxiliassem na perquirição criminal.

Essas são algumas das formas de preservação das provas obtidas no meio digital. Importante, agora, entender melhor como são propriamente obtidas as evidências virtuais, outro desafio enfrentado na investigação.

3.2 DOS MEIOS PARA OBTENÇÃO DE DADOS PELA POLÍCIA JUDICIÁRIA

A investigação criminal é a fase em que a polícia judiciária viabiliza formas de obtenção de evidências e busca da verdade real sobre determinada notícia crime recebida. É nessa fase que ocorrem os mandados, os pedidos de prisões preventivas e as quebras de sigilo quando necessário para a melhor investigação e preservação de provas.

No meio digital, no entanto, sabe-se que as evidências possuem um caráter muito mais temporário que o mundo real. Além disso, a capacidade evasiva do cibercriminoso é bem maior do que o criminoso comum, aquele que pratica crimes de maneira presencial e física. Isso se dá pela alta velocidade e transmissões de informações que ocorrem no meio virtual. Para o cibercriminoso, evadir-se sem deixar rastros é uma tarefa fácil, pois o agente já possui conhecimento técnico para isso e sabe que a autoridade policial ainda depende de aparato estatal e capacitação técnica para investigá-lo.

No entanto, apesar da sensação de anonimato e da complexidade das investigações, o cibercriminoso pode ser sim encontrado e as provas do seu ato ilícito preservadas como evidências no seu processo judicial. Os termos a seguir estão previstos no art. 5º e incisos da Lei nº 12.965/2/14, conhecida como Marco Civil da Internet.

Primeiramente, têm-se os administradores de Sistema Autônomo, que são os provedores de internet, como, por exemplo, a Oi, a Vivo, NET, dentre outros. Por

[47] HTTRACK WEBSITE COPIER. **Free Software offline browser.** Disponível em: https://www.httrack.com/page/1/en/index.html. Acesso em: 09 nov. 2020.

meio deles é que são distribuídos os endereços de IP (*Internet Protocol*), que são um conjunto de algarismos que identificam e diferenciam determinado dispositivo conectado à internet. É também com eles que se pode ter acesso aos registros de conexão, os quais determinam data, hora de início e término de uma conexão, sua duração e localização.

As aplicações de internet se referem ao "conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet", ou seja, sites, aplicativos, redes sociais, dentre outros. Por meio dessas aplicações, ficam armazenadas as informações de login, como data e hora de sua utilização, os quais ficam vinculados ao endereço de IP.

É por meio do IP que se diferenciam os usuários de determinada aplicação. Seria como o documento de identidade do usuário. Com o IP, pode-se saber, por fim, o conteúdo acessado pelo usuário e consequentemente suas ações na rede mundial de internet. O que fez enquanto acessava determinada aplicação, a que momento e de que local.

Esses dados são fornecidos pelos provedores, os chamados administradores de Sistema Autônomo e não há necessidade de autorização judicial para que sejam informados, apenas a requisição da autoridade policial. Nas palavras de Barreto, Silva e Kufa "o fornecimento desses registros evita o anonimato e, consequentemente, atribui a cada conteúdo uma autoria certa e determinada"[48].

Entretanto, o fornecimento desses dados sem a autorização judicial deve ser visto com cautela, uma vez que essas informações servem, em um primeiro momento, apenas para identificar suspeitos, e não o conteúdo que o agente acessou no momento da conexão em si. Esse entendimento tem sido alvo de grande discussão ainda na doutrina brasileira. Há quem diga que, apesar de os dados poderem ser solicitados diretamente pela autoridade policial, o pedido deve vir munido já de uma especificação do usuário, ou seja, uma identificação prévia do agente. O que se conseguiria com os dados, em verdade, seria uma confirmação de que o suspeito estava nas imediações do crime ou conectado ao IP que realizou o delito (se por meio digital, no caso).

---

[48] BARRETO, Alessandro Gonçalves; KUFA, Karina; SILVA, Marcelo Mesquita. **Cibercrimes e Seus Reflexos no Direito Brasileiro**. Salvador: Editora Juspodivm, 2020.

Os pedidos de informações de dados de IP são fundamentados, principalmente, no artigo 10, § 3º, da Lei nº 12.965/14[49], que refere:

> 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.
> (...)
> § 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.

Muitos provedores têm se negado a fornecer essas informações baseando-se na ideia de que esses pedidos são incompatíveis com a Constituição Federal, pois ferem direitos fundamentais como o da privacidade. Além disso, esse repasse de informações se trataria de uma quebra de sigilo de dados, que necessita ordem judicial, e também na crítica ao pedido "genérico" e sem alvo específico. As autoridades policiais já têm solicitado, por via judicial, a quebra de sigilos para evitar as negações dos provedores e aplicações de internet. No entanto, ainda há uma resistência no fornecimento de dados, havendo o acionamento de Tribunais para confirmar a ordem[50].

A exemplo disso, cita-se um caso parecido que trouxe o assunto aos Tribunais brasileiros. Em Sergipe, o Tribunal de Justiça do Estado, por maioria dos votos, manteve decisão que obrigava a Google a fornecer dados sobre um grupo de pessoas que teriam estado em um local próximo onde houve um homicídio em determinado dia e intervalo de tempo.

Resumidamente, um capitão da Polícia Militar de Sergipe foi assassinado na cidade de Porto da Folha, no mesmo estado, e durante a investigação foi solicitado a quebra de sigilo de dados, a qual foi deferida, determinando ao Google que fornecesse os dados de conexão, acesso às aplicações de internet, dentre outras

---

[49] BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Congresso Nacional [2014]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 08 nov. 2020.

[50] FILHO, Demócrito Reinaldo. Limites e requisitos da ordem judicial para quebra de sigilo de dados armazenados por provedor de serviços na internet: Desnecessidade de individualização prévia do(s) investigado(s) e do esgotamento de outros meios de prova. **Jus,** Teresina, mar. 2020. Disponível em: https://jus.com.br/artigos/80222/limites-e-requisitos-da-ordem-judicial-para-quebra-de-sigilo-de-dados-armazenados-por-provedor-de-servicos-na-internet/3. Acesso em: 29 mai. 2021.

informações de pessoas que estivessem próximas ao local indicado, na hora e data especificados, utilizando os serviços da empresa. A gigante da tecnologia impetrou mandado de segurança contra a ordem, alegando, basicamente, as controvérsias anteriormente citadas.

Entretanto, o TJSE[51] negou o pedido da Google, entendendo que a decisão do juiz singular encontra respaldo no artigo 22 do Marco Civil da Internet, que prevê o seguinte:

> Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.

Além disso, o pedido era limitado às informações de conexão e acesso às aplicações de internet, e não ao seu conteúdo. Em seu voto, a Relatora Desembargadora Iolanda Santos Guimarães frisou que o sistema "o sistema jurídico diferencia a tutela dada ao conteúdo das comunicações mantidas entre indivíduos e às informações de conexão e de acesso a aplicações de internet, garantindo uma maior proteção ao primeiro e flexibilizando a proteção da segunda".

Em verdade, conforme pontua Demócrito Reinaldo Filho[52], é até ilógico o requerimento dos provedores de que a autoridade indique suspeitos ao requererem os dados, uma vez que o propósito da quebra desse sigilo é justamente a busca da autoria delitiva, ou seja, a identidade da pessoa que fez uso dos serviços ou acessou uma determinada aplicação. Além disso, o art. 22 do Marco Civil da Internet não tem como exigência a necessidade de indicação, por parte da autoridade requerente, dos eventuais alvos.

---

[51] SERGIPE. Tribunal de Justiça do Estado de Sergipe. **Acórdão nº 201818567**. Mandado de Segurança Cível. Processo 201800111901. Constitucional e Processo Penal. Mandado de Segurança. Inquérito policial. Investigação do homicídio do Comandante da Companhia Independente de Operações Policiais Especiais em área de Caatinga (CIOPAC). Decisão que determina a quebra de sigilo telemático [...]. Impenetrante: Google Brasil Internet LTDA; Google LLC; Impetrado: Juízo de Direito da Comarca de Porto da Folha. Relatora: Des. Iolanda Santos Guimarães, 22 de agosto de 2018. Disponível em: https://www.conjur.com.br/dl/tj-quebra-sigilo-generica-baseada-tempo.pdf. Acesso em: 20 abr. 2021.

[52] FILHO, Demócrito Reinaldo. Limites e requisitos da ordem judicial para quebra de sigilo de dados armazenados por provedor de serviços na internet: Desnecessidade de individualização prévia do(s) investigado(s) e do esgotamento de outros meios de prova. **Jus,** Teresina, mar. 2020. Disponível em: https://jus.com.br/artigos/80222/limites-e-requisitos-da-ordem-judicial-para-quebra-de-sigilo-de-dados-armazenados-por-provedor-de-servicos-na-internet/3. Acesso em: 29 mai. 2021.

Não obstante, ainda segundo o autor, os provedores e aplicações de internet não possuem legitimidade para contestar ordens judiciais baseadas no direito à privacidade dos usuários, tendo em vista que não são representantes deles. Nesse sentido, um usuário que se sinta ofendido na sua esfera íntima de privacidade pode, individualmente, propor ações defendendo seus direitos, mas não o seu provedor de internet ou aplicações que utiliza.

Ademais, necessário observar que quaisquer informações e elementos recebidos de terceiros que não tenham ligação ou não representem utilidade para com a investigação devem ser descartados e, obviamente, protegidos. Ou seja, os dados pessoais das pessoas não envolvidos no objeto da ordem continuam confidenciais, de modo que sua violação ou vazamento configura, inclusive, crime.

Apesar do arcabouço legislativo referente à obtenção de provas e o entendimento favorável das cortes em obrigar às empresas de tecnologia de informar os dados solicitados pelas autoridades, a legislação material penal brasileira ainda padece de uma melhoria significativa em termos de repressão da criminalidade cibernética.

3.3 AS LIMITAÇÕES DA LEGISLAÇÃO PENAL BRASILEIRA

Apesar de o Brasil demonstrar comprometimento e preocupação com o mundo digital com a criação de normas com diretrizes do uso da internet no país, como a Lei Geral de Proteção de Dados e o Marco Civil da Internet, citadas anteriormente, o mesmo não se pode dizer quanto ao combate da criminalidade virtual. Isto é, a quantidade de normas que criminalizam condutas que deveriam ser consideradas criminosas são pouquíssimas.

É princípio básico do ordenamento jurídico o de anterioridade da lei penal, previsto, inclusive, no art. 1º do Código Penal Brasileiro. Por meio dele, não se considera crime a ação ou omissão que não esteja tipificada e, consequentemente, não há punição. Nesse ínterim, havendo poucas normas que tratem de delitos cibernéticos, o Brasil corre risco de se tornar paraíso do cibercriminoso.

Na verdade, já houve até mesmo decisão do STF[53] no sentido de que a carência de norma penal sobre crime cibernético serviu como fundamento para o indeferimento de ordem cautelar de prisão e extradição:

> EXTRADIÇÃO – PRISÃO CAUTELAR – PLEITO FORMULADO PELA INTERPOL – POSSIBILIDADE – INOVAÇÃO INTRODUZIDA PELA LEI Nº 12.878/2013 – DELITO INFORMÁTICO (CRIME DIGITAL): "INVASÃO DE DISPOSITIVO INFORMÁTICO" (CP, ART. 154-A, ACRESCIDO PELA LEI Nº 12.737/2012) – **FATO DELITUOSO ALEGADAMENTE COMETIDO, EM TERRITÓRIO AMERICANO (ESTADO DO TEXAS), EM 2011 – CONDUTA QUE, NO MOMENTO EM QUE PRATICADA (2011), AINDA NÃO SE REVESTIA DE TIPICIDADE PENAL NO ORDENAMENTO POSITIVO BRASILEIRO – O SIGNIFICADO JURÍDICO DO PRINCÍPIO CONSTITUCIONAL DA RESERVA DE LEI EM MATÉRIA DE TIPIFICAÇÃO E DE COMINAÇÃO PENAIS (CF, ART. 5º, INCISO XXXIX) – "NULLUM CRIMEN, NULLA POENA SINE PRAEVIA LEGE" – DUPLA TIPICIDADE (OU DUPLA INCRIMINAÇÃO): CRITÉRIO QUE REGE O SISTEMA EXTRADICIONAL – NECESSIDADE DE QUE O FATO SUBJACENTE AO PEDIDO DE EXTRADIÇÃO (OU AO PLEITO DE PRISÃO CAUTELAR PARA EFEITOS EXTRADICIONAIS) ESTEJA SIMULTANEAMENTE TIPIFICADO , NO MOMENTO DE SUA PRÁTICA, TANTO NA LEGISLAÇÃO PENAL DO BRASIL QUANTO NA DO ESTADO ESTRANGEIRO – PRECEDENTES – SITUAÇÃO INOCORRENTE NO CASO, POIS A CONDUTA PUNÍVEL IMPUTADA AO SÚDITO ESTRANGEIRO RECLAMADO SOMENTE PASSOU A SER CONSIDERADA CRIMINOSA, NO BRASIL, EM ABRIL DE 2013** (QUANDO SE ESGOTOU O PERÍODO DE "VACATIO LEGIS" DA LEI Nº 12.737/2012, ART. 4º), POSTERIORMENTE, PORTANTO, À DATA EM QUE FOI ELA ALEGADAMENTE PRATICADA NOS ESTADOS UNIDOS DA AMÉRICA – EVOLUÇÃO DO TRATAMENTO LEGISLATIVO, NO BRASIL, PARA FINS PENAIS, DOS CRIMES INFORMÁTICOS – OCORRÊNCIA, AINDA, NA ESPÉCIE, DE OUTRO OBSTÁCULO JURÍDICO: DELITO INFORMÁTICO (OU CRIME DIGITAL, OU INFRAÇÃO PENAL CIBERNÉTICA) SEQUER PREVISTO NO ARTIGO II DO TRATADO DE EXTRADIÇÃO BRASIL/EUA – ROL EXAUSTIVO, FUNDADO EM "NUMERUS CLAUSUS", QUE DEFINE, NO CONTEXTO BILATERAL DAS RELAÇÕES EXTRADICIONAIS ENTRE BRASIL E EUA, OS CRIMES QUALIFICADOS PELA NOTA DE "EXTRADITABILIDADE" – PRECEDENTES, A ESSE RESPEITO, DO SUPREMO TRIBUNAL FEDERAL – CONSEQUENTE IMPOSSIBILIDADE DE PROCESSAR-SE DEMANDA EXTRADICIONAL FUNDADA EM DELITO ESTRANHO AO ROL TAXATIVO INSCRITO NO ARTIGO II

[53] BRASIL. Supremo Tribunal Federal (2. Turma). **Questão de Ordem na Prisão Preventiva para Extradição 732.** Extradição. Prisão Cautelar. Pleito formulado pela Interpol. Possibilidade. Inovação introduzida pela lei nº 12.878/2013. Delito Informático (crime digital): "Invasão de dispositivo informático". Relator: Min. Celso de Mello, 11 de novembro de 2014. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=7645112. Acesso em: 12 abr. 2021.

> DESSE TRATADO DE EXTRADIÇÃO – NATUREZA JURÍDICA DO TRATADO DE EXTRADIÇÃO (“LEX SPECIALIS”) – PRECEDÊNCIA JURÍDICA , QUANTO À SUA APLICABILIDADE, SOBRE O ORDENAMENTO POSITIVO INTERNO DO BRASIL – “PACTA SUNT SERVANDA ” – PRECEDENTES – A INADMISSIBILIDADE DA EXTRADIÇÃO (CAUSA PRINCIPAL) TORNA INVIÁVEL O ATENDIMENTO DO PEDIDO DE PRISÃO PREVENTIVA (MEDIDA REVESTIDA DE CAUTELARIDADE E IMPREGNADA DE CARÁTER ANCILAR E MERAMENTE ACESSÓRIO) – QUESTÃO DE ORDEM QUE SE RESOLVE NO SENTIDO DO INDEFERIMENTO DO PEDIDO DE PRISÃO CAUTELAR. (Grifou-se)

Em virtude dessa situação e considerando o tempo de criação do Código Penal ainda vigente (mais de 80 anos), foi criado um projeto de lei que está tramitando no Senado Federal que visa à criação de um novo Código Penal. O PLS 236/2012[54], de autoria do Senador José Sarney (MDB/AP), prevê a reforma do Código Penal de 1940, com a modificação de várias áreas do direito penal e, uma delas, é a criação de uma parte especial no novo Código para tratar dos delitos cibernéticos.

Apesar de não abordar todas as hipóteses possíveis de delitos cibernéticos, o Projeto de Lei já mostra um avanço na criação de normas que positivem comportamentos inadequados na rede mundial de computadores. Além disso, o artigo 208 do Projeto de Lei traz importantes conceitos para tratar dos crimes cibernéticos, como sistemas informáticos, dados informáticos, provedor de serviços e dados de tráfego. No entanto, apenas dois delitos cibernéticos foram criados (artigos 209 e 210 do Projeto de Lei[55]) e que apresentam penas brandas, sendo eles:

> **Acesso indevido**
> Art. 209. Acessar, indevidamente ou sem autorização, por qualquer meio, sistema informático protegido, expondo os dados informáticos a risco de divulgação ou de utilização indevida:
> Pena: prisão, de seis meses a um ano, ou multa.
> **Sabotagem informática**
> Art. 210. Interferir de qualquer forma, indevidamente ou sem autorização, na funcionalidade de sistema informático ou de comunicação de dados informáticos, causando-lhe entrave, impedimento, interrupção ou perturbação grave, ainda que parcial:
> Pena – prisão, de um a dois anos.

[54] BRASIL. Senado Federal. **Projeto de Lei do Senado nº 236/2012.** Anteprojeto de Código Penal. Brasília, DF: Senador Federal [2012]. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=3515262&ts=1613697834640&disposition=inline. Acesso em: 26 mar. 2021.
[55] Ibid.

Observe-se que ambos os casos possuem penas que chegam, ao máximo, dois anos, sendo que uma delas até admite multa como opção de pena ao julgador. Além disso, por possuírem penas máximas cominadas que não ultrapassem os dois anos, ambos os delitos são considerados crimes de menor potencial ofensivo, o que implica a judicialização destes perante o Juizado Especial Criminal, regido pela Lei 9.099/95[56]. Por meio dela, ainda, é permitida ao agente a aplicação da transação penal.

Em termos de criminologia, talvez os institutos despenalizadores como os previstos na lei dos Juizados Especiais sejam uma ótima opção, uma vez que a pena privativa de liberdade é considerada a forma mais extrema de controle penal[57], enquanto as restritivas de direito uma forma de readequar condutas sem a privação de liberdade. No entanto, as consequências do crime podem ser extremamente danosas, conforme amplamente debatido no presente trabalho, e a transação penal não parece apresentar uma reprimenda necessária ao delito.

Cite-se, por exemplo, alguém que invada um dispositivo informático privado e protegido e obtenha segredos comerciais e industriais, por exemplo. O agente se enquadraria no parágrafo terceiro do art. 209, que prevê a modalidade qualificada do crime, elevando a pena para, no mínimo, um e, no máximo, dois anos. Esse criminoso ainda estaria abrangido pelo Juizado Especial Criminal, mesmo que tenha retirado informações que gere prejuízo gigantesco a uma empresa privada.

Outro exemplo claro é o ataque hacker sofrido pelo Tribunal de Justiça do Rio Grande do Sul, que foi citado anteriormente. A invasão do sistema, por si só, apesar do grande prejuízo financeiro e às investigações em curso, trariam ao criminoso penas que não ultrapassassem dois anos, se não houver a possibilidade de associar a conduta criminosa a outro tipo penal.

Os crimes citados no Projeto de Lei apresentam também hipóteses de qualificadora e majorantes das penas. Contudo, ainda assim, as penas não chegam a um patamar necessário para reprimenda do crime. Além disso, ambos os delitos são condicionados à representação da vítima, exceto nos casos em que a administração pública seja a vítima.

---

[56] BRASIL. **Lei nº 9.099, de 26 de setembro de 1995.** Dispõe sobre os Juizados Especiais Cíveis e Criminais e dá outras providências. Brasília, DF: Congresso Nacional [1995]. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9099.htm. Acesso em: 29 mar. 2021.

[57] BARATTA, Alessandro. **Criminologia Crítica e Crítica do Direito Penal**. 2 ed. Rio de Janeiro: Freitas Bastos, 1999.

Não obstante, o fato de esses delitos estarem, em sua maioria, abarcados pela competência do Juizado Especial Criminal, ou seja, judicializado conforme a Lei 9.099/95[58], prejudica muito as investigações. Isso porque crimes de menor potencial ofensivo, ao serem apurados pela autoridade policial, são feitos, geralmente, por meio de um termo circunstanciado[59]. Diferentemente do Inquérito Policial, o termo circunstanciado é um meio de apuração mais simplificado, seguindo princípios de celeridade, oralidade, informalidade e economia processual, o que não torna o procedimento apropriado à investigação do crime cibernético, uma vez que, como já visto, a apuração de autoria e a obtenção de provas são complexas e tendem a levar um certo tempo.

É claro que nada obsta a autoridade de instaurar o Inquérito Policial para investigação de delitos, mesmo aqueles de menor potencial ofensivo, conforme entendimento jurisprudencial já pacificado[60]. Entretanto, o fato de o legislador ter enquadrado os delitos cibernéticos em penas menores que dois anos significa que o fez por considerar os crimes cibernéticos delitos de menor potencial ofensivo, que seriam abarcados pelos juizados especiais criminais, cujos principais princípios processuais são o da informalidade e o da celeridade. Ou seja, as infrações cibernéticas prescindiriam de uma investigação robusta, com provas periciais complexas e, muitas vezes, quebras de sigilo.

Aliás, há quem defenda que os procedimentos no âmbito dos Juizados Especiais sequer admitem provas periciais, o que é imprescindível na investigação dos delitos cibernéticos. Nesse sentido, o seguinte Enunciado do FONAJE[61] (Fórum Nacional de Juizados Especiais):

---

[58] BRASIL. **Lei nº 9.099, de 26 de setembro de 1995.** Dispõe sobre os Juizados Especiais Cíveis e Criminais e dá outras providências. Brasília, DF: Congresso Nacional [1995]. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9099.htm. Acesso em: 29 mar. 2021.

[59] Art. 69 da Lei 9.099/95 - A autoridade policial que tomar conhecimento da ocorrência lavrará termo circunstanciado e o encaminhará imediatamente ao Juizado, com o autor do fato e a vítima, providenciando-se as requisições dos exames periciais necessários.
BRASIL. **Lei nº 9.099, de 26 de setembro de 1995.** Dispõe sobre os Juizados Especiais Cíveis e Criminais e dá outras providências. Brasília, DF: Congresso Nacional [1995]. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9099.htm. Acesso em: 29 mar. 2021.

[60] BRASIL. Superior Tribunal de Justiça (6. Turma). **Habeas Corpus nº 41.348 - SP**. Penal e Processual. Habeas Corpus substitutivo de Recurso Ordinário. Crime de Usura. Inquérito Policial. Ausência de Justa Causa. Lei 9.000/95. Possibilidade de instauração de inquérito Policial. Denegação da Ordem. Relator: Min. Hélio Quaglia Barbosa, 02 de agosto de 2005. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/1805102/habeas-corpus-hc-41348-sp-2005-0013966-9/inteiro-teor-12957410. Acesso em: 29 mar. 2021.

[61] CONSELHO NACIONAL DE JUSTIÇA. **Enunciados Cíveis**. Brasília, DF: CNJ, [20--]. Disponível em: https://www.cnj.jus.br/corregedoria-nacional-de-justica/redescobrindo-os-juizados-especiais/enunciados-fonaje/enunciados-civeis/. Acesso em: 29 mar. 2021.

> ENUNCIADO 54 – A menor complexidade da causa para a fixação da competência é aferida pelo objeto da prova e não em face do direito material.

Pela mesma linha, diversos estados brasileiros, por meio dos seus tribunais e associações de magistrados, também entenderam pela impossibilidade de perícia técnica nos Juizados Especiais, por exemplo a APAMAGIS (Associação Paulista de Magistrados)[62] e o Tribunal de Justiça Gaúcho[63]. Especificamente quanto aos delitos cibernéticos, a seguinte decisão do Tribunal de Justiça do Paraná[64]:

> CONFLITO NEGATIVO DE COMPETÊNCIA CRIME – SUPOSTA OCORRÊNCIA DO CRIME PREVISTO NO ARTIGO 154-A, DO CÓDIGO PENAL - JUÍZO COMUM E JUIZADO ESPECIAL – AUTORIA DESCONHECIDA – NECESSIDADE DE QUEBRA DE SIGILO DE DADOS CADASTRAIS DOS E-MAILS UTILIZADOS PELA VÍTIMA – COMPETÊNCIA DO JUÍZO COMUM DEVIDO À COMPLEXIDADE DO FEITO – CONFLITO DE COMPETÊNCIA PROCEDENTE. (...) Assim, verifica-se que a autoria do delito é desconhecida, o que torna necessário uma maior dilação probatória, com a realização de perícias, procedimentos estes que não se coadunam com a realidade dos Juizados Especiais. (...)

Atualmente, com a recente entrada em vigor da Lei 14.155/2021, a qual se falará mais à frente, o crime cibernético do art. 154-A previsto no Código Penal é um exemplo da ciência do legislador da complexidade e gravidade do delito, deixando ele de ser judicializado pela Lei nº 9.099/95, tendo em vista sua alteração no texto e elevação das penas.

Assim, no caso dos delitos cibernéticos, é nítida a complexidade da investigação e da necessidade de uma prova pericial robusta, inclusive com pedidos de interceptações telemáticas, instrumentos que não são admitidos perante os Juizados Especiais. Portanto, a perquirição criminal dos crimes digitais deveria ser

---

[62] ASSOCIAÇÃO PAULISTA DE MAGISTRADOS. **Enunciados do Fórum de Juizados Especiais do Estado de São Paulo (FOJESP)**: Minuta consolidada em 12/06/2018. São Paulo: APAMAGIS, 2018. Disponível em: https://apamagis.com.br/institucional/fojesp/. Acesso em: 29 mar. 2021.

[63] RIO GRANDE DO SUL. Tribunal de Justiça do Estado do Rio Grande do Sul. **Cartilha dos Juizados Especiais Cíveis**. Porto Alegre: Tribunal da Justiça, [20--]. Disponível em: https://www.tjrs.jus.br/novo/institucional/1o-grau/juizados-especiais/cartilha-dos-juizados-especiais/. Acesso em: 29 mar. 2021.

[64] PARANÁ. Tribunal de Justiça do Paraná. **Conflito de Competência Crime nº 1.392.910-3.** Relator Convidado: Benjamim Acácio de Moura e Costa, 06 de novembro de 2015. Disponível em: https://tj-pr.jusbrasil.com.br/jurisprudencia/255319428/conflito-de-jurisdicao-cj-13929103-pr-1392910-3-decisao-monocratica/inteiro-teor-255319444. Acesso em: 29 mar. 2021.

realizada por meio de Inquérito Policial, procedimento pelo qual diligências complexas podem ser realizadas e requeridas, respeitando uma formalidade que não é vista com os termos circunstanciados.

3.3.1 A LITERALIDADE DO ART. 154-A DO CÓDIGO PENAL E A LEI Nº 14.155/2021

Outro fato importante a se analisar quanto à limitação da legislação penal brasileira é a descrição fática dos dispositivos, em especial o art. 154-A, do Código Penal[65], um dos únicos delitos cibernético positivado no referido diploma. O delito mencionado entrou no Código Penal por meio da Lei nº 12.737/2012[66], conhecida como “Lei Carolina Dieckmann”, pelo fato da grande repercussão diante do caso[67] da atriz que batizou o nome da lei ter seus equipamentos eletrônicos invadidos e seus arquivos pessoais divulgados sem autorização, inclusive fotos íntimas que se tornaram virais nas redes sociais. O ocorrido levou a uma intensa pressão social para a criminalização desses tipos de condutas que não possuíam enquadramento no Código Penal.

Recentemente, no dia 27 de maio de 2021, o Presidente da República, Jair Bolsonaro, aprovou a Lei nº 14.155[68], que alterou o Código Penal Brasileiro, reescrevendo o artigo em comento e tornando mais severa a sua pena, além de criar modalidades específicas do crime de furto e estelionato quando praticados por meio eletrônico.

---

[65] BRASIL. **Decreto-lei nº 2.848, de 7 de dezembro de 1940.** Código Penal. Brasília, DF: Congresso Nacional [1940]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 29 ago. 2020.

[66] BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, DF: Congresso Nacional [2012]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 29 ago. 2020.

[67] CAROLINA Dieckmann fala pela 1ª vez sobre fotos e diz que espera 'justiça': Atriz deu entrevista a Patricia Poeta no Jornal Nacional desta segunda (14). Trinta e seis fotos pessoais dela foram publicadas na internet. **G1,** São Paulo, 15 mai. 2012. Disponível em: http://g1.globo.com/pop-arte/noticia/2012/05/carolina-dieckmann-fala-pela-1-vez-sobre-roubo-de-fotos-intimas.html. Acesso em: 05 abr. 2021.

[68] BRASIL. **Lei nº 14.155, de 27 de maio de 2021**. 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. Brasília, DF: Congresso Nacional [2021]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso em: 29 mai. 2021.

Anteriormente, previa o crime de Invasão de Dispositivo Informático (art. 154-A do Código Penal) o seguinte:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

Atualmente, a redação do artigo, com a alteração promovida pela nova Lei, assim prevê o delito:

> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.

Além disso, aumentou também a majoração das penas quando o crime for cometido em situações específicas e alterou a pena quando o delito tem como resultado uma das hipóteses do parágrafo terceiro:

> §2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico.
>
> §3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
>
> Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa

O objeto jurídico do crime, como se percebe, é a privacidade individual e profissional que contêm dados armazenados em dispositivos informáticos. A tipificação do crime é mais uma forma de assegurar o direito fundamental previsto na Constituição Federal, no art. 5º, inciso X, que prevê a inviolabilidade da intimidade, vida privada, honra e imagem das pessoas, assegurando-se o direito de indenização pelo dano decorrente de sua violação.

A descrição inicial da conduta do art. 154-A, anterior à nova lei, recebeu diversas críticas de juristas por não apresentar, de forma completa, as hipóteses

cabíveis para tipificação do crime. Embora a nova redação tenha solucionado um dos maiores problemas na interpretação, alguns continuam existindo. Uma dessas críticas recai no fato de que o legislador estabeleceu a conduta criminosa no ato da invasão sem autorização do dono do dispositivo, mas não sobre as informações contidas. Nesse sentido, havendo mais de uma pessoa utilizando o dispositivo, por exemplo, seus dados contidos lá ficam sob autorização do real dono do aparelho.

Conforme explica Rogério Sanches Cunha[69],

> Há, no entanto, uma crítica sobre a forma como o legislador tratou essa situação, pois o tipo penal estabelece a conduta criminosa no ato de invasão sem autorização expressa ou tácita do dispositivo, não das informações. O ideal seria, diante da possibilidade de que mais de um indivíduo utilize o dispositivo informático, que a tutela recaísse expressamente no titular das informações armazenadas.

Rogério Sanches Cunha também critica a falta de previsão no excesso no cometimento do crime, isto é, uma vez autorizado o acesso ao dispositivo, se o agente for além do que foi autorizado, o crime não se verifica, como, por exemplo, nos casos em que o dono do dispositivo autoriza “um técnico a acessar uma pasta com fotografias, mas ele vai além e obtém outras informações armazenadas no dispositivo.” Nesse caso, não haverá crime, pois essa conduta não está abrangida no tipo penal, que pressupõe uma violação de dispositivo.

É, também, nesse sentido a maioria das críticas ao texto da Lei. Mesmo com a nova alteração, o referido artigo continua possuindo uma divergência doutrinária em relação ao núcleo do tipo, isto é, alguns doutrinadores entendem que a norma apresenta duas condutas, quais sejam, a de “invadir” e a de “instalar”, como refere Guilherme de Souza Nucci[70]. Já para Rogério Greco[71] e Cezar Roberto Bitencourt[72], o núcleo seria apenas o ato de “Invadir”, sendo o “instalar” um ato secundário, originária da conduta de invadir.

Como se vê, a redação do artigo traz uma interpretação dúbia: Há duas condutas previstas ou apenas uma com agir alternativos? Entretanto, nas duas

---

[69] CUNHA, Rogério Sanches, **Manual de Direito Penal:** Parte Especial (arts. 121 ao 361). 11. ed. Salvador: JusPODIVM, 2019.
[70] NUCCI, Guilherme de Souza. **Código Penal Comentado**. 14. ed. Rio de Janeiro: Forense, p. 813-813, 2014.
[71] GRECO, Rogério. **Código Penal Comentado**. 8. ed. Niterói: Impetus, p. 470, 2014.
[72] BITENCOURT, Cezar Roberto. **Código Penal Comentado**. 8. ed. São Paulo: Saraiva, p. 680, 2014.

hipóteses, certo é que o objetivo do agente é o mesmo: obter vantagem ilícita. Mas aqui reside outro problema: imagina-se que uma pessoa invada dispositivo ou instale vulnerabilidade sem intenção de obter vantagem ilícita, mas por simples vontade de prejudicar alguém por não gostá-la, por exemplo. Segundo Fernando Capez e Stela Prado[73], essa previsão no tipo penal acaba desvirtuando o crime, tendo em vista que o crime, como anteriormente mencionado, tutela a privacidade da pessoa, e não o patrimônio, como seria no caso exemplificado.

Além disso, antes da alteração no texto da norma, o dispositivo informático que não possui mecanismo de segurança não podia ser objeto material das ações incriminadas, uma vez que o delito exige a "violação indevida de mecanismo de segurança". Assim, invadir ou instalar vulnerabilidades em dispositivos que não continham mecanismos de segurança (como senhas, por exemplo) não configurariam o crime descrito no art. 154-A. Essa situação e interpretação da norma abriu precedentes para que criminosos pudessem invadir dispositivos que não continham senhas e conseguiriam obter, adulterar ou destruir dados sem que essa conduta receba uma punição estatal.

Felizmente, com a recente alteração trazida pela Lei nº 14.155/2021, o trecho que referia a necessidade de mecanismo de segurança para configuração do crime foi retirado e, assim, bens sem proteção de senha também encontram respaldo na normal legal. Entretanto, as diversas interpretações doutrinárias quanto ao texto continuam existindo.

3.3.2 OS PANORAMAS DAS LEIS 12.737/12 E 12.735/12

Conforme anteriormente citado, a Lei nº 12.737 de 2012, conhecida como "Lei Carolina Dieckmann", foi uma tentativa do legislador de tipificar criminalmente condutas que visem à invasão de dispositivos informáticos. Na mesma data de sua aprovação, também foi aprovada a Lei 12.735 de 2012[74], que dispõe sobre a estruturação de setores e equipes de polícia judiciária especializadas no combate à

[73] CAPEZ, Fernando; PRADO, Stela. **Código Penal Comentado**. 5. ed. São Paulo: Saraiva, p. 347, 2014.

[74] BRASIL. **Lei nº 12.735, de 30 de novembro de 2012**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Brasília, DF: Congresso Nacional [2012]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 29 ago. 2020.

ação criminosa por meio da rede de computadores, dispositivos de comunicação e sistema informatizado.

É indiscutível que a tecnologia tem como principal objetivo facilitar a vida das pessoas e não seria diferente com a polícia judiciária em termos de investigação. É por esse motivo que a informatização dos processos judiciais tem se tornado a realidade no país e tem deixado o processo físico para trás. Na mesma lógica, a criação de departamentos de polícia especializados no combate ao crime digital se faz necessário diante da complexidade do *modus operandi* dos agentes criminosos.

Assim, também foi instituído o Inquérito Policial eletrônico, em que diligências, perícias e outros meios de prova são acondicionados e realizados eletronicamente, por meio de um sistema que confira autenticidade, integridade e confiabilidade, além de constante atualização do sistema, nos moldes em que também foi constituído o processo judicial eletrônico pela Lei nº 11.419 de 2006. Nesse ínterim, tornou-se mais ágil, fácil, simplificada e segura a obtenção e reunião de provas da fase inquisitorial, abrindo mão do papel físico.

Apesar disso, existem diversas críticas em relação à criação das duas leis. Segundo Josefa Cristina Kunrath[75]:

> Há quem defenda que os diplomas legislativos Lei n.º 12.735/2012 e Lei n.º 12.737/2012 foram editados com a pretensão de preencher o vazio normativo existente na legislação penal brasileira, de modo que, os novos tipos penais são suficientes para reprimir as condutas ilícitas mais recorrentes praticadas por meio das redes informáticas. Por outro lado, há o posicionamento, segundo o qual, a tipificação criminal de delitos informáticos através da Lei n.º 12.737/2012 deixa de fora do alcance da legislação penal alguns importantes ataques cibernéticos, para os quais não há previsão legal.

É no sentido do último posicionamento, por exemplo, o entendimento do Ministério Público de São Paulo (MPSP)[76], ao publicar nota sobre a edição das referidas leis em seu site:

---

[75] KUNRATH, Josefa Cristina Tomaz Martins. **A expansão da criminalidade no ciberespaço:** desafios de uma política criminal de prevenção ao cibercrime. 158 f. il. 2014. Dissertação (Mestrado) — Faculdade de Direito, Universidade Federal da Bahia, Salvador, p. 97, 2014.

[76] SÃO PAULO (Estado). Ministério Público do Estado de São Paulo. Centro de Apoio Operacional Criminal. **Nova lei de crimes cibernéticos entra em vigor.** São Paulo: MPSP, [2013]. Disponível em: http://www.mpsp.mp.br/portal/page/portal/cao_criminal/notas_tecnicas/NOVA%20LEI%20DE%20CRIMES%20CIBERN%C3%89TICOS%20ENTRA%20EM%20VIGOR.pdf. Acesso em: 05 abr. 2021.

> Como visto, a Lei nº 12.737/2012, embora represente certo avanço ao tipificar crimes cibernéticos propriamente ditos, contém inúmeras deficiências e confrontos com o sistema penal e processual penal vigente, o que deve merecer a atenção dos aplicadores. Os crimes cibernéticos propriamente ditos são a porta de entrada para outras condutas criminosas, facilitando a utilização do computador como instrumento para cometer delitos. O legislador não contemplou a invasão de sistemas, como os de clouding computing, optando por restringir o objeto material àquilo que denominou dispositivo informático, sem, contudo, defini-lo. Atividades de comercialização de cracking codes e de engenharia reversa de software também não foram objeto da norma. Além das imperfeições na redação dos tipos, as penas cominadas na nova lei são ínfimas se considerada a potencial gravidade das condutas incriminadas, bastando dizer que um ataque de denegação de serviço pode colocar em risco vidas de uma população inteira. Implicam, por outro lado, a competência do Juizado Especial Criminal, cujo procedimento sumaríssimo é incompatível com a complexidade da investigação e da produção da prova de crimes de alta tecnologia (perícia no dispositivo informático afetado, por exemplo). Numa síntese, os tipos e penas da Lei nº 12.737/2012 não conseguem dar as respostas esperadas pela Sociedade para desestimular aqueles que abusam das facilidades tecnológicas.

Por outro lado, há defensores que dizem que os crimes cometidos por meio digital podem ser enquadrados nos tipos penais já existentes no ordenamento, uma vez que, na maioria das vezes, os criminosos apenas se valem do meio digital como meio para o resultado do crime. O que seria, de fato, necessário, na verdade, para esses defensores, seria um aparato tecnológico e maior investimento na área para desenvolvimento e capacidade das polícias e órgãos.

Entretanto, essa opção do legislador de não ter tipificado outras condutas se baseia numa política criminal, muito pelo fato de que o art. 154-A, apesar de estabelecer uma conduta criminosa e uma pena, é utilizado como meio do infrator, o que acarreta em sua consunção. Contudo, para alguns juristas, essa carência de normas inviabiliza também o combate ao crime cibernético.

Dessa forma, a ausência de tipificação penal de diversas condutas e o enquadramento dos delitos já previstos como de menor potencial ofensivo gera certa insegurança jurídica e uma deficiência na proteção Estatal. Sobre os diplomas legais mencionados, Patricia Peck Pinheiro e Victor Auilo Haikal afirmam[77]:

---

[77] PINHEIRO, Patrícia Peck; HAIKAL, Victor Auilo. A nova lei de crimes digitais. **Gazeta do Povo**, [*s.l.*], 11 abr. 2013. Disponível em: https://www.gazetadopovo.com.br/vida-publica/justica-direito/artigos/a-nova-lei-de-crimes-digitais-evf935c0vqjw7rh9b4cq75tfy. Acesso em: 05 abr. 2021.

> Essas leis não esgotaram os tipos penais digitais, pois é impossível que não se considere como crime a indisponibilidade de sistemas de informação de entidades privadas, como sites de comércio eletrônico ou bancos, ou a disseminação de vírus e outros códigos maliciosos, em razão da sociedade inteira estar cada vez mais interconectada.
> Também não houve cuidado do legislador ao indicar que a invasão necessita de obtenção, modificação ou exclusão de dados, pois a bisbilhotagem ou envio de dados para terceiros podem desviar do tipo penal, além de considerar que invadir dispositivo sem mecanismo de segurança também não é crime. Sem mencionar que a falta de obrigação de guarda de logs de conexão e acesso pode inviabilizar a instrução criminal pela dificuldade em se identificar o agente.
> Por fim, para que haja proveito da lei para a proteção dos seus dispositivos, é indispensável utilizar proteção com senha, código ou dados biométricos para impedir o acesso não autorizado. Isso vale para computadores de mesa, notebooks, tablets, smartphones e reprodutores de áudio ou vídeo portáteis. É importante deixar um sistema de firewall ou detecção de intrusão sempre ativo e com perfil de atividades maliciosas sempre atualizado e refinado para evitar falsos positivos.

A falta desses elementos nas normas nacionais implica em um agravamento da complexidade de investigação dos crimes cibernéticos. O fato de existirem normas que visem ao combate dessa modalidade criminosa já apresenta um avanço do Brasil em busca da garantia da ordem pública e segurança nacional. Entretanto, a tipificação penal de algumas condutas ainda precisa ser reconhecida, uma vez que muitas ações criminosas são cometidas por meio eletrônico e sequer possuem uma norma que as condene. Não se trata aqui de um viés punitivista, com inobservância da *ultima ratio* da lei penal, mas sim de uma preocupação com a impunidade de condutas prejudiciais e que muitas sequer são de conhecimento dos usuários de dispositivos eletrônicos.

A Convenção de Budapeste separa um capítulo inteiro sobre normas de direito penal material que os países signatários devem considerar para internalizar nos seus ordenamentos jurídicos. Assim, com a adesão à Convenção o Brasil passaria a se comprometer em criar tipificações penais que, de fato, promovam um eficaz combate aos crimes cibernéticos, bem como adotaria políticas criminais eficientes na prevenção dos delitos informáticos. Não obstante, também se comprometeria a atuar junto à comunidade internacional na repressão dessa modalidade criminosa, como se verá agora.

4 A COOPERAÇÃO JURÍDICA INTERNACIONAL E A CONVENÇÃO DE BUDAPESTE COMO MECANISMOS ESSENCIAIS NA INVESTIGAÇÃO DOS CRIMES CIBERNÉTICOS

A Cooperação Jurídica Internacional é um instrumento auxiliador dos Estados para assegurar o funcionamento da Justiça em seus territórios, “por meio da qual um Estado, para fins de procedimento no âmbito da sua jurisdição, solicita a outro Estado medidas administrativas ou judiciais que tenham caráter judicial em pelo menos um desses Estados.”[78] Esse instituto está, inclusive, previsto na Constituição Federal, no seu artigo 4º, inciso IX, que prevê a “cooperação entre os povos para o progresso da humanidade”. Não se trata, portanto, de uma mera ajuda voluntária ou compromisso moral, mas sim, de uma obrigação jurídica[79].

Assim, por ser, de fato, uma obrigação jurídica, não há razão para se sustentar que a cooperação internacional enfraquece a soberania de um país. Cumpre destacar que a relativização da soberania estatal não está relacionada ao enfraquecimento do Estado diante demais países, mas, pelo contrário, a cooperação internacional está ligada, na verdade, ao papel de cumprimento de obrigações por parte do Estado com seus nacionais e demais países. A ofensa à soberania, portanto, não pode ser usada como justificativa de um país para cometer violações de direitos e deveres dentro do seu território.

A cooperação internacional já é realidade entre a maioria dos países do mundo. São diversas as iniciativas que fomentaram as alianças entre países em diversas áreas de atuação, especialmente no mútuo combate aos diversos tipos de crimes que ocorrem transnacionalmente. Não especificamente aos crimes cibernéticos, mas alguns acordos de cooperação internacional abriram portas para a desburocratização, facilitando a comunicação entre autoridades, o que permite uma comunicação mais rápida, dentre outros benefícios. Cita-se, por exemplo, a Força Tarefa Global, criada em 2003 para combater a pornografia infantil, o Grupo de Ação

---

[78] BRASIL. Ministério da Justiça. **Cartilha de Cooperação Jurídica Internacional em Matéria Penal**. Brasília, DF: Ministério da Justiça, 2014. Disponível em: https://www.justica.gov.br/sua-protecao/lavagem-de-dinheiro/institucional-2/publicacoes/arquivos/cartilha-penal-09-10-14-1.pdf. Acesso em: 12 abr. 2021.

[79] TOFFOLI, José Antonio Dias; CESTARI, Virgínia Charpinel Junger. Mecanismos de Cooperação Jurídica Internacional no Brasil. *In*: BRASIL. Ministério da Justiça. **Manual de Cooperação Jurídica Internacional e Recuperação de Ativos**: Cooperação em Matéria Civil. Brasília, DF: Ministério da Justiça, 2008.
Disponível em: https://www.tjdft.jus.br/publicacoes/edicoes/manuais/manuais-da-corregedoria/2009Manual_CooperacaoCivil.pdf. Acesso em: 12 abr. 2021.

Financeira sobre Lavagem de Dinheiro e o Financiamento ao Terrorismo (GAFI/FATF), “cujo propósito é desenvolver e promover políticas nacionais e internacionais de combate à lavagem de dinheiro e ao financiamento do terrorismo”[80]; a Europol, serviço europeu de polícia, que trabalha com o intercâmbio de informações criminais entre os países da União Europeia, especialmente o cibercrime e o terrorismo[81]; a Interpol, também um serviço de polícia e que coopera com quase 200 países[82], dentre outros.

No Brasil, a Autoridade Central é um órgão do Ministério da Justiça e é o responsável pela condução da cooperação internacional. Compete a ela “receber, analisar, adequar, transmitir e acompanhar o cumprimento dos pedidos de cooperação jurídica.”[83] Além disso, a Autoridade Central também busca junto à comunidade internacional melhorias no sistema de cooperação internacional jurídica entre os Estados.

A Autoridade Central é dividida em dois departamentos, sendo eles o Departamento de Estrangeiros (DEEST), pelo qual compete analisar e tramitar os pedidos de extradição e deportação, e o Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional (DRCI), pelo qual se analisa e tramitam os demais pedidos oriundos de cooperação jurídica internacional, nos termos do Decreto nº 9.662/19. A investigação dos crimes transnacionais é de competência da Polícia Federal, a teor do previsto no artigo 109, inciso V, da Constituição Federal.

Ainda, a Cooperação Internacional está prevista em tratados e acordos bilaterais e multilaterais com diversos países. Por meio desses instrumentos, o Brasil não apenas adquire o direito de solicitar cooperação jurídica de outros países, como também se compromete a dar cumprimento aos pedidos realizados pelos mesmos.

---

[80] GOVERNO FEDERAL. Conselho de Controle de Atividades Financeiras. **Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo (Gafi/FATF)**. Brasília, DF: Governo Federal [20--]. Disponível em: https://www.gov.br/coaf/pt-br/atuacao-internacional/prevencao-e-combate-a-lavagem-de-dinheiro-e-ao-financiamento-do-terrorismo/gafi. Acesso em: 06 jun. 2021.

[81] EUROPOL. **About Europol.** Haia: Europol, [20--]. Disponível em: https://www.europol.europa.eu/about-europol. Acesso em: 06 jun. 2021.

[82] INTERPOL. **What is INTERPOL?** Lion: INTERPOL, [20--]. Disponível em: https://www.interpol.int/Who-we-are/What-is-INTERPOL. Acesso em: 06 jun. 2021.

[83] BRASIL. Ministério da Justiça. **Cartilha de Cooperação Jurídica Internacional em Matéria Penal**. Brasília, DF: Ministério da Justiça, 2014. Disponível em: https://www.justica.gov.br/sua-protecao/lavagem-de-dinheiro/institucional-2/publicacoes/arquivos/cartilha-penal-09-10-14-1.pdf. Acesso em: 12 abr. 2021.

Segundo a lição de Barreto, Kufa e Silva[84], a cooperação jurídica internacional possui uma classificação adotando os seguintes três critérios: “iniciativa da solicitação, qualidade de quem coopera e procedimento.” A iniciativa da solicitação se refere a quem está solicitando o auxílio, podendo ser ativo ou passivo, respectivamente requerente e requerido. A qualidade está relacionada à entidade ou instituição que está solicitando e à instituição solicitada, ou seja, as autoridades judiciais, no caso da cooperação jurídica, ou não judiciais, nos casos das autoridades administrativas. E, por último, o procedimento, como o próprio nome sugere, diz respeito à forma com que será solicitado o auxílio, seja por pedido de extradição, auxílio direto, carta rogatória, dentre outros.

No que se refere à natureza, Raúl Cervini observa três teorias, conforme citado por Barreto[85], sendo a primeira uma jurisdição própria, vinculada ao requerido com o processo em curso no Estado requerente; a segunda uma delegação de jurisdição feita pelo requerente ao requerido e a terceira, em que a cooperação seria um mecanismo que se submete a uma ordem jurídica internacional, ou seja, os Estados em cooperação sofrem uma “influência determinante dos tratados internacionais”.

A última parece a mais razoável a ser adotada entre Estados cooperadores, pois é por meio dela que se chega a um “padrão universal de garantias”[86], isto é, a produção de provas e instrução processual em diferentes sistemas legislativos pode ser dificultoso ao internalizar, no Estado requerente, por exemplo, a prova produzida no estrangeiro. Para Bechara, também citado por Barreto[87]:

> A observância das garantias que integram o processo justo constitui o modelo garantista na atividade probatória, ou seja, o padrão ou *standard* obrigatório que deve ser respeitado na definição do procedimento probatório no plano abstrato e normativo, assim como na atividade dos sujeitos processuais. Na hipótese da prova produzida no exterior, a diversidade entre os sistemas é superada pelo reconhecimento do padrão normativo universal das garantias processuais, as quais se posicionam como *standard* universal e demandam dos Estados solicitados um esforço de verificação quanto

---

[84] BARRETO, Alessandro Gonçalves; KUFA, Karina; SILVA, Marcelo Mesquita. **Cibercrimes e Seus Reflexos no Direito Brasileiro**. Salvador: Editora Juspodivm, p. 109, 2020.
[85] Ibid., p. 54-55, Apud CERVINI, Raúl; TAVAREZ, Juarez. **Princípios de Cooperação Judicial Penal Internacional no Protocolo do Mercosul**. São Paulo: Revista dos Tribunais, 2000.
[86] Ibid.
[87] Ibid., p. 93, Apud BECHARA, Fábio Ramazzini. **Cooperação Jurídica Internacional em Matéria Penal:** Eficácia da Prova Produzida no Exterior. São Paulo: Saraiva, 2011.

> à equivalência e compatibilidade da regulação interna com esses valores, resguardando, assim, a eficácia da prova a ser produzida.

Ainda segundo Bechara, as garantias processuais mínimas que são necessárias para estabelecer o padrão universal mencionado seriam o direito à prova, à presunção de inocência, ao contraditório, igualdade de armas, à defesa, à razoável duração do processo, à assistência gratuita do intérprete, respeito à vida privada, intimidade e inviolabilidade do domicílio. Essas garantias, portanto, devem ser observadas pelos Estados cooperadores, garantindo que se estabeleça um padrão de valores preservados por eles, independente do seu Direito interno, assim como os direitos fundamentais. Ressalta-se que isso não quer dizer que a forma procedimental pela qual será feita a cooperação precise, necessariamente, ser idêntica, mas que tão somente os Estados observem o padrão de garantias universais.

Assim, tem-se que aos pedidos de assistência internacional, segundo Barreto, a lei material aplicada será a do Estado requerente, em virtude do princípio da territorialidade, mas a lei processual gera certa controvérsia. De regra, segundo o Código de Bustamante, a prerrogativa é do Estado requerido, mas diretrizes internacionais não estipulam uma regra para tanto, ficando a escolha a cargo dos Estados. Assim, o ideal, conforme Bechara, seria que as partes elegessem a lei processual do Estado requerente, evitando que as provas produzidas possam ser passíveis de vícios com o procedimento, sempre “respeitando os princípios basilares do Estado requerido”.

Quanto ao crime cibernético, conforme amplamente debatido nesse estudo, trata-se de uma modalidade complexa de delito. Sua característica de ocorrência à distância e em locais diversos, podendo ser simultaneamente inclusive de forma transnacional, torna extremamente difícil sua investigação, preservação de provas e consequentemente a atribuição da autoria delitiva. O mundo digital, além de tudo, é um mundo fragmentado politicamente, com leis e estruturas governamentais distintas e que não obedece a fronteiras físicas. Em especial, no Brasil, o problema se agrava ainda mais pela carência de tipificação penal de condutas criminosas no meio virtual, como visto anteriormente.

O cibercrime, embora sua gravidade e característica transnacional, não possui amparo diante o Tribunal Penal Internacional (TPI), que apenas processa e

julga casos limitados a genocídios, crimes de guerra e contra a humanidade. E isso muito se dá em decorrência de diversos obstáculos envolvendo interesses políticos, religiosos e econômicos dos Estados, o que dificulta também a criminalização de condutas.

Segundo Barreto, Kufa e Silva,[88]

> Para a criação de uma efetiva justiça criminal internacional, faz-se necessária a existência de quatro elementos: um ordenamento jurídico para definir os tipos penais, força policial para investigar tais delitos, um sistema judiciário para aplicar a lei a um caso concreto e um sistema prisional para punir ou recuperar os condenados. Em razão dessas instituições não existirem, em nível internacional, com a independência e o alcance existente em níveis domésticos, o sistema penal internacional não pode ser pensado como o interno, formado pela interação e sobreposição de diferentes instituições e ordenamentos, dificultando sua efetividade e abrangência.

Nesse sentido, não há como combater o cibercrime em escala mundial sem a mútua-ajuda internacional. Pensando nisso e cientes da grande incidência de ataques aos usuários da Internet e da constante ocorrência dos crimes virtuais, diversos países já buscam formas de cooperação internacional no combate e repressão aos delitos cibernéticos, motivo pelo qual foi realizada a Convenção de Budapeste, que determinou diversas diretrizes aos Estados-membros que assinaram o tratado.

4.1 AS DIFICULDADES DA COOPERAÇÃO INTERNACIONAL

Apesar da criação da Convenção de Budapeste ser um marco importante para o combate e resolução dos crimes cibernéticos, ela, por si só, não afasta todas as dificuldades envolvidas na investigação interacional. A burocracia, morosidade do judiciário e falta de pessoal capacitado, além do aumento da criminalidade tornam a investigação muito mais complexa do que o normal, desafios estes que não apenas o Brasil enfrenta. Diante de tal contexto, novas medidas devem ser analisadas e criadas para facilitar a cooperação e investigação.

---

[88] BARRETO, Alessandro Gonçalves; KUFA, Karina; SILVA, Marcelo Mesquita. **Cibercrimes e Seus Reflexos no Direito Brasileiro**. Salvador: Editora Juspodivm, p. 93, 2020. Apud BECHARA, Fábio Ramazzini. Cooperação Jurídica Internacional em Matéria Penal: Eficácia da Prova Produzida no Exterior. São Paulo: Saraiva, 2011.

O auxílio direto, apesar de não ter previsão constitucional como a carta rogatória, é um instrumento que vem sendo utilizado com mais frequência entre os Estados. Isso se dá pelo fato de o auxílio direto ser um mecanismo muito semelhante à carta rogatória, mas difere pelo fato de não precisar ser requerido por autoridade judicial estrangeira, mas, sim, administrativa, a outra autoridade administrativa nacional. Ou seja, não é necessário o exequatur.

Sobre o auxílio direto, Dias Toffoli[89] diz que

> Com o incremento das relações globais e a disseminação dos crimes transnacionais, percebeu-se que os mecanismos clássicos de cooperação jurídica internacional eram inaplicáveis ou ineficientes em determinadas situações. Para fazer face às novas demandas, os Estados se viram diante da necessidade de criar mecanismos mais arrojados que viabilizassem a cooperação jurídica, preservando, ao mesmo tempo, sua celeridade e segurança. Surge, assim, o que se convencionou chamar de pedido de Auxílio Direto.

Ainda assim, o auxílio direto deve ser requerido por meio da autoridade central. No entanto, o instituto do auxílio direto se traduz menos burocrático que a carta rogatória, mas não menos válido, uma vez que esse ato é praticado por autoridade nacional, "afastando qualquer argumento de invasão, supressão ou afronta à soberania nacional."[90] Além disso, o auxílio direto respeita os princípios constitucionais e a legislação infraconstitucional, especialmente os tratados e acordos bilaterais. Observa-se que, no entanto, o auxílio direto também possui alguns problemas com a burocracia, assim como as cartas rogatórias, como a tramitação física, tradução e a instrução dos pedidos entre os órgãos.

Barreto ainda defende que a cooperação jurídica internacional deva passar por uma mudança de fase, pela qual se verá uma maior informalidade, celeridade e eficiência no processamento. Segundo o autor, uma das soluções para facilitar o envio da cooperação seria o "uso de sistemas eletrônicos para envio, recebimento e processamento das cartas rogatórias", além da desnecessidade do exequatur por um Tribunal Superior. Dessa forma, o juízo destinatário final da solicitação poderia

---

[89] TOFFOLI, José Antonio Dias; CESTARI, Virgínia Charpinel Junger. Mecanismos de Cooperação Jurídica Internacional no Brasil. *In*: BRASIL. Ministério da Justiça. **Manual de Cooperação Jurídica Internacional e Recuperação de Ativos**: Cooperação em Matéria Civil. Brasília, DF: Ministério da Justiça, 2008. Disponível em: https://www.tjdft.jus.br/publicacoes/edicoes/manuais/manuais-da-corregedoria/2009Manual_CooperacaoCivil.pdf. Acesso em: 12 abr. 2021.

[90] BARRETO, Alessandro Gonçalves; KUFA, Karina; SILVA, Marcelo Mesquita. **Cibercrimes e Seus Reflexos no Direito Brasileiro**. Salvador: Editora Juspodivm, p. 120, 2020.

processar o pedido mais rapidamente, havendo possibilidade de recurso direito ao STJ das decisões tomadas, se necessário.

O auxílio direto também não deveria ter uma intermediação por meio da autoridade central, uma vez que é característico do instrumento a tentativa de desburocratização e celeridade no pedido. Barreto ainda defende a desnecessidade de tramitação desses pedidos pelos meios consulares, bastando que as autoridades envolvidas no pedido de cooperação estejam previamente cadastradas em um meio eletrônico que os permita uma comunicação segura e garantindo a confiabilidade, autenticação, autorização, integridade dos dados e privacidade.

Todo esse panorama pode se fazer real e concreto com a colaboração entre os Estados e também a colaboração entre o poder público e privado, sobretudo as empresas de tecnologia, uma vez que possuem estrutura e capacidade econômica para auxiliar nas investigações e repressão dos crimes cibernéticos.

Outro quesito que se deve levar em consideração quanto às dificuldades da cooperação internacional reside no fato de existirem fatores quantos aos países cooperadores que influenciam na forma que ela ocorre. De acordo com Hufnagel (2012), citado por Barreto (2020)[91], existem quatro fatores:

> Em primeiro lugar, a gravidade do crime transnacional em foco desempenha um papel importante. Isso não implica, todavia, que quanto maior a problemática, mais próximo será a cooperação. Isso porque, em segundo lugar, o grau de cooperação mútua promovida por Estados também depende muito de como, e se, eles percebem a gravidade do problema da mesma maneira e em mesmo nível. Se eles concordam que o problema é sério, então, obviamente, haverá maior chance de se expandir ou intensificar sua cooperação. Caso não haja esta comunhão de percepção da gravidade, haverá pouca chance de que a cooperação floresça. Em terceiro lugar, o grau de cooperação é determinado por outro fator que repousa nos simples interesses políticos e econômicos dos Estados. Estes interesses podem induzir os Estados a cooperar, ainda que não considerem o problema urgente, porque isso será propício para relações mútuas. Em quarto lugar, deve notar-se que os Estados podem estar preocupados com a manutenção da ordem pública e da segurança em sua vizinhança e, portanto, sentirem-se obrigados, por exemplo, em estabelecer cooperação policial e tratados de assistência jurídica aos países vizinhos.

[91] BARRETO, Alessandro Gonçalves; KUFA, Karina; SILVA, Marcelo Mesquita. **Cibercrimes e Seus Reflexos no Direito Brasileiro**. Salvador: Editora Juspodivm, p. 120, 2020. Apud HUFNAGEL, Saskia; HARFIELD, Clide; BRONITT, Simon. **Cross-border Law Enforcement, Regional Law Enforcement Cooperation:** European, Australian and Asia-Pacific perspectives. New York: Routledge, 2012. p. 3.

Em outras palavras, quando se fala de cooperação jurídica internacional, está-se diante da colaboração entre dois ou mais Estados, os quais cada um possui suas particularidades, sua própria cultura, crenças e necessidades, bem como estrutura jurídica diferente. Assim, o que pode ser visto como grave em um Estado, não necessariamente terá a mesma proporção em outro. E isso se deve a diversas razões, como os interesses políticos, econômicos e culturais.

Por esses motivos que os tratados e convenções desempenham papel importante na internalização ao ordenamento jurídico nacional. É por meio deles que os países assinantes reconhecem a problemática e cooperam juntos para sua solução de forma homogênea. Além disso, representam também uma forma de garantia da segurança nacional, pois, como citado, problemas que ocorrem em países fronteiriços (e até mesmo os que não são) podem acabar se tornando problemas, mais tarde, do Estado vizinho. Não obstante, esses acordos também apresentam uma harmonização entre as legislações (tanto de direito material como processual) sobre determinado assunto, o que favorece uma cooperação mais fácil, célere e ágil.

É claro que cada país ostenta sua própria estrutura policial e judicial para o combate ao crime. Hufnagel, citado novamente por Barreto[92], ainda refere a necessidade de "conhecimento e a imersão nos fundamentos das estruturas e culturas dos sistemas penais estrangeiros envolvidos". Isso torna a cooperação jurídica muito mais eficaz, uma vez que possibilita a criação de agências especiais e destinação de recursos para a repressão de delitos.

Atrelado a isso, importante destacar ainda que muitos dos delitos informáticos possuem criptomoedas como pagamento aos criminosos. As criptomoedas são moedas digitais e fazem parte de um fluxo de riquezas aquém do sistema financeiro e bancário tradicional. Há países, inclusive, que as consideram ilegais, outros as aceitam como forma legal de pagamento e outros que as classificam como bens materiais, como é o caso do Brasil[93]. Suas características principais e motivo de uso por criminosos é o fato de que as criptomoeadas são totalmente digitais,

---

[92] BARRETO, Alessandro Gonçalves; KUFA, Karina; SILVA, Marcelo Mesquita. **Cibercrimes e Seus Reflexos no Direito Brasileiro**. Salvador: Editora Juspodivm, p. 120, 2020. Apud HUFNAGEL, Saskia; HARFIELD, Clide; BRONITT, Simon. **Cross-border Law Enforcement, Regional Law Enforcement Cooperation:** European, Australian and Asia-Pacific perspectives. New York: Routledge, 2012. p. 3.

[93] Segundo a Receita Federal, em 2021, as moedas virtuais são consideradas como "Bens ou Serviços", conforme códigos 81, 82 e 89 na declaração de imposto de renda anual.

transacionadas por meio de criptografia e ainda não possuem regulamentação na maioria dos países do mundo, o que dificulta o controle e rastreamento das operações[94], segundo dados do estudo "O aumento da popularidade das criptomoedas e da atividade criminosa associada"[95].

Dessa forma, as negociações envolvendo as criptomoedas também podem ocorrer de diferentes partes do globo. Apenas com a cooperação jurídica internacional é que será possível um engajamento de países para rastrear essas operações, bem como também na investigação dos crimes virtuais e, para isso, a Convenção da Budapeste representa um papel importante.

4.2 A CONVENÇÃO DE BUDAPESTE

Criada em 2001, os Estados membros do Conselho da Europa, juntamente de outros países, que hoje totalizam sessenta e dois signatários, realizaram a Convenção de Budapeste para criar uma política criminal comum de combate e repressão aos delitos "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"[96].

Sua criação denota uma necessidade de frear uma constante e crescente onda de ataques virtuais aos internautas da rede mundial de computadores, bem como uma adequação e uniformização de legislações dos países contra essas condutas criminosas. Além disso, pelo caráter transnacional do cibercrime, a jurisdição de cada país poderia interferir nas investigações, pois a simples coleta de dados poderia ser encarada como uma violação à soberania territorial do país onde se tem o alvo das investigações. Nesse contexto, a Convenção de Budapeste surge para erradicar esses conflitos territoriais, harmonizar a legislação sobre a matéria,

---

[94] PETRY, Guilherme. Blockchain do crime: como investigar crimes com criptomoedas. **The Hack,** [*s.l.*], dez. 2020. Disponível em: https://thehack.com.br/blockchain-do-crime-como-investigar-crimes-com-criptomoedas/. Acesso em: 29 mai. 2021.

[95] No original: "The Rise in Popularity of Cryptocurrency and Associated Criminal Activity". KETHINENI, Sesha; CAO, Ying. The Rise in Popularity of Cryptocurrency and Associated Criminal Activity. **Sage Journals**, v. 30, n. 3, set. 2020. DOI: https://doi.org/10.1177/1057567719827051. Disponível em: https://journals.sagepub.com/doi/abs/10.1177/1057567719827051. Acesso em: 13 abr. 2021.

[96] BRASIL. Ministério Público Federal. **Convenção Sobre o Cibercrime.** Budapeste, 23 nov. 2001. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf. Acesso em: 29 ago. 2020.

melhorar técnicas de combate e repressão aos delitos e buscar uma cooperação jurídica internacional entre os países assinantes.

O documento é separado por capítulos e aborda, em cada um, diferentes temas, com orientações para uniformizar as medidas adotadas pelos países signatários ao elaborarem seus respectivos projetos de lei. Destaca-se no texto do tratado a preocupação com as mudanças provocadas pelo advento do mundo digital e a globalização, que acarretam no uso desse meio para o cometimento de delitos, além do reconhecimento da necessidade de parcerias entre o Poder Público e a iniciativa privada, mormente as empresas de tecnologia, e também a divulgação da necessidade de cooperação entre os Estados-membros, a fim de estabelecer uma política criminal mais célere e eficaz.

Da mesma forma, a Convenção abalizou os bens jurídicos tutelados, quais sejam, o da segurança da informação e vida privada dos usuários da rede, a confidencialidade, integridade e disponibilidade de sistemas informáticos, bem como a necessidade de criminalização de condutas fraudulentas dentro desses sistemas. A notabilidade de uma coordenação no combate do crime cibernético é tão grande que o Conselho da Europa vem estudando a criação de uma agência especial com o intuito de garantir que países assinantes da Convenção tenham acesso a contato que auxilie nas investigações desses crimes. Essa agência ainda seria capaz de mostrar a importância da aderência de outros países à Convenção, bem como seria responsável pela coleta de dados sobre a ocorrência de crimes cibernéticos, podendo elaborar relatórios que auxiliem no desenvolvimento de novas políticas criminais.

Em dezembro de 2020 foi criado o Centro Europeu de Competência em Cibersegurança (ENISA), sediado na Romênia, que constitui “o principal instrumento da União Europeia (UE) para reunir investimentos em investigação e desenvolvimento tecnológico e industrial na área da cibersegurança.”[97] A UE tem investido fortemente em políticas de cibersegurança e também no combate e repressão de crimes informáticos, com a criação de um centro europeu

[97] CONSELHO EUROPEU. **O novo Centro Europeu de Competências em Cibersegurança ficará instalado em Bucareste, na Roménia**. Bruxelas: Conselho Europeu, 10 dez. 2020. Disponível em: https://www.consilium.europa.eu/pt/press/press-releases/2020/12/10/the-new-european-cybersecurity-competence-centre-to-be-located-in-bucharest-romania/#:~:text=O%20Centro%20de%20Compet%C3%AAncias%20em,industrial%20na%20%C3%A1rea%20da%20ciberseguran%C3%A7a. Acesso em: 13 abr. 2021.

especializado em cibercriminalidade, que faz parte da Europol para ajudar os países da UE na investigação e desmonte de organizações criminosas, além de outras medidas que visam a segurança dos usuários da internet, como regras e políticas relacionados com a justiça e aplicação da lei, acesso às provas eletrônicas, encriptação e conservação de dados.[98]

Ainda, sobre a Convenção de Budapeste, ela se divide em quatro capítulos, sendo o primeiro deles sobre as terminologias, rechaçando o significado de sistemas informáticos, dados informáticos, dentre outros termos para melhor interpretação das normas. O segundo diz respeito às medidas que os países devem adotar dentro do seu território, especificamente quanto à tipificação penal, além de estabelecer os bens jurídicos tutelados. O terceiro trata da cooperação internacional, estabelecendo princípios gerais, e o quarto e último trata das disposições finais.

Sobre direito material, o tratado tipifica os crimes contra sistemas e dados informáticos, computadores, pornografia infantil e violações de direitos autorais. Importante destacar que a Convenção considera cibercrime apenas condutas dolosas, ou seja, a hipótese culposa não está presente em nenhum momento. Isso porque não se parece razoável processar e condenar alguém por ter repassado um e-mail com vírus sem intenção, por exemplo, tendo em vista que a maioria dos usuários da internet sequer possui conhecimento técnico específico para perceber o *malware* ao que se está exposto. Em sede de direito processual, fala sobre condições de preservação e conservação de dados, bem como busca e apreensão, recolhimento em tempo real de dados informáticos e a interceptação, além da competência e cooperação internacional.

Quanto ao Direito Penal material, previsto a partir do artigo 2º da Convenção, parece que o Brasil, com o implemento do artigo 154-A do Código Penal, tentou preencher as diretrizes contidas na Convenção. Isso porque no artigo 2º da Convenção está previsto a adoção pelos países assinantes de “medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, o acesso intencional e ilegítimo à totalidade ou a parte de um sistema informático”.

---

[98] CONSELHO EUROPEU. **Cibersegurança:** como combate a UE as ciberameaças. Bruxelas: Conselho Europeu, 21 abr. 2021. Disponível em: https://www.consilium.europa.eu/pt/policies/cybersecurity/. Acesso em: 13 abr. 2021.

Entretanto, a Convenção ainda prevê outras hipóteses de delitos cibernéticos, como a interceptação ilegítima, prevista no artigo 3º, que diz respeito à violação da privacidade de comunicações; a interferência de dados, prevista no artigo 4º, que se refere ao ato de deteriorar, danificar, eliminar, apagar ou alterar dados de programas informáticos, como a instalação de vírus, por exemplo; e interferência de sistemas, prevista no artigo 5º, que se refere ao impedimento da utilização legítima de sistemas informáticos, como os serviços de telecomunicação. No tangente ao artigo 6º, que prevê o uso abusivo de dispositivos, ou seja, a produção, comercialização e obtenção de dispositivos ou programas informáticos para cometer os delitos anteriormente citados, percebe-se que ele já está previsto no parágrafo 1º do artigo 154-A do Código Penal, porém, condicionada ao cometimento exclusivo deste. Frisa-se que estas hipóteses são previstas apenas na sua forma dolosa.

Os artigos 7º e 8º da Convenção fazem parte do Título 2, que fala das infrações relacionadas a computadores. O artigo 9º, do Título 3, refere-se às infrações relacionas à pornografia infantil, e o artigo 10º, do Título 4, diz respeito às infrações com violações de direito autoral. Em teste, são delitos que geralmente já estão disciplinados e positivados nos ordenamentos jurídicos dos países.

Os artigos 7º e 8º da Convenção se referem à falsidade informática e à Burla informática, respectivamente. No Brasil, apesar de não estarem assim nomeados, o crime de falsidade informática tem relação com os crimes de falsidade previstos no Código Penal. Por meio desse artigo, pune-se a conduta do agente que crie ou altere, de forma não autorizada, dados armazenados de forma virtual. Esses dados possuem algum valor jurídico, de forma que sua alteração pode trazer consequências nas relações jurídicas[99]. Alguém que falsifique uma assinatura eletrônica, por exemplo, seria enquadrado neste artigo.

No tocante ao artigo 8ª da Convenção, que trata da Burla informática, essa se refere ao crime cometido com manipulação da entrada em sistema informático com o fim de “efetuar transferência de propriedade ilegal”[100], ou seja, burlar o sistema objetivando a perda de bens de terceiros, o que também poderia se enquadrar no disposto do artigo 154-A do Código Penal.

---

[99] BRASIL. Ministério Público Federal. **Minuta do Relatório Explicativo**. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/coordenacao/comissoes-e-grupos-de-trabalho/combate-crimes-cirberneticos/convention-on-cybercrime/explanatory-reports_pt.pdf. Acesso em: 06 jun. 2021.
[100] Ibid.

Dispositivos sobre pornografia infantil, como antes já analisado, estão previstas no ordenamento jurídico brasileiro, conforme artigos 240 e seguintes do Estatuto da Criança e do Adolescente e artigo 218-C do Código Penal, bem como delitos contra a propriedade intelectual, previstos no Título III, Capítulo I, do Código Penal, e na Lei nº 9.279/96. Entretanto, quanto aos crimes de propriedade intelectual, salienta-se a ausência de norma interna que trate da engenharia reversa de software, prática em que o agente se utiliza de uma análise estrutural do código de um determinado programa ou aplicativo para descobrir como ele funciona. Em que pese seja utilizada em pesquisas e fins acadêmicos, pode ser uma ação com intuito criminoso, como a sua utilização na pirataria para burlar a proteção anticópia[101].

Sobre a matéria processual, a Convenção busca adaptar as medidas processuais clássicas, como a busca e apreensão no ambiente eletrônico, por exemplo, além de apresentar novas medidas que auxiliam nas investigações, tendo em vista a volatilidade dos dados. Assim, o Título 2 apresenta as medidas legislativas e outras necessárias que os países que aderiram à Convenção devem tomar para o efetivo processamento legal dos crimes cibernéticos.

Nos artigos 16 e 17 da Convenção está prevista a preservação expedita de dados informatizados armazenados, ou seja, são dados já armazenados por fornecedores de serviços e que devem ser preservados por eles, especialmente aqueles que “existem motivos para pensar que os mesmos são suscetíveis de perda ou alteração”[102]. O artigo 18 trata da habilitação das autoridades dos países com poderes necessários para obrigar uma pessoa que se encontre no seu território a fornecer dados armazenados especificados, ou um fornecedor de serviços que ofereça seus serviços no território de uma das Partes, a prestar informações.

O artigo 19 diz respeito à busca e apreensão no meio virtual, de modo que o país assinante do tratado se compromete em “adaptar” sua legislação, permitindo a busca e apreensão ou poder equivalente para conseguir dados informatizados. Importante destacar que, nesse caso, a busca e apreensão ocorre dentro do próprio território, sendo vedada “a busca e apreensão transfronteiriça sem recorrer às

---

[101] HAUTSCH, Oliver. O que é engenharia reversa? **Tecmundo**, [*s.l.*], 28 set. 2009. Disponível em: https://www.tecmundo.com.br/pirataria/2808-o-que-e-engenharia-reversa-.htm. Acesso em: 06 jun. 2021.

[102] BRASIL. Ministério Público Federal. **Convenção Sobre o Cibercrime.** Budapeste, 23 nov. 2001. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf. Acesso em: 29 ago. 2020.

modalidades tradicionais de assistência mútua”[103]. Além disso, em caso de dificuldade na investigação de acesso ao dado informatizado ou sua interpretação, ainda há a possibilidade de recorrer ao administrador que forneceu os dados para auxiliar nesse caso, não se impedindo uma medida coercitiva se necessário.

Os artigos 20 e 21 se referem ao poder das autoridades competentes de obterem dados em tempo real, tanto quanto dados relativos ao tráfego, como de seu conteúdo. E por fim, o artigo 22º prevê a competência e jurisdição, que já foi abordado anteriormente quando se falou da extraterritorialidade do crime cibernético.

Algumas das diretrizes processuais elencadas na Convenção de Budapeste já são observadas pelo Direito interno no Brasil, como o que ocorre com as interceptações telefônicas, de dados, medidas coercitivas, dentre outras hipóteses. São apenas instruções que a maioria dos países já possuem em seu ordenamento nacional. O diferencial da Convenção está, de fato, atrelado na cooperação jurídica internacional e auxílio mútuo entre os países.

Em especial, uma das atribuições previstas na Convenção está no Artigo 35º, do Título 3 do Capítulo III, que dispõe sobre a criação de uma rede que funcione 24 horas por dia, durante os sete dias da semana: a Rede 24 por 7.

A criação dessa rede vem com o intuito de tornar mais célere e eficaz o contato entre as nações durante a investigação dos crimes digitais. Isto é, os canais de cooperação internacional, antes da ferramenta, não apresentavam tanta eficácia quanto a Rede 24/7, que também visa à preservação das evidências.

Assim, sobre a Rede 24/7, explicam Alesandro Barreto e Beatriz Brasil[104]:

> Essa rede é composta por pontos de contato nos países, disponíveis 24 horas por dia e sete dias por semana, os quais se comunicam diretamente e da forma mais rápida possível (e-mail, telefone, etc.) e posteriormente formalizam o procedimento através de preenchimento de um pedido formal de cooperação.
> Esses pontos de contato devem garantir a prestação de assistência imediata, aconselhamento técnico, preservação e recolhimento de dados, bem como a prestação de informações necessárias à elucidação do fato e ainda à localização de suspeitos. Sem essa

[103] BRASIL. Ministério Público Federal. **Minuta do Relatório Explicativo**. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/coordenacao/comissoes-e-grupos-de-trabalho/combate-crimes-cirberneticos/convention-on-cybercrime/explanatory-reports_pt.pdf. Acesso em: 06 jun. 2021.
[104] BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silvera. **Manual de Investigação Cibernética: à Luz do Marco Civil da Internet**. Rio de Janeiro: Editora Brasport, 2016.

> coleta e compartilhamento de informações, a cooperação tornar-se-ia limitada e, as vezes, impossível.

A criação da Rede 24/7 é um grande avanço no combate do crime cibernético, pois proporciona às autoridades de outros países acesso mais ágil às provas e investigações sob jurisdição estrangeira. Além disso, a Convenção ainda assegura que os assinantes do tratado devem garantir pessoas capacitadas para atender as solicitações para o melhor funcionamento do sistema.

Além da Rede 24/7, o artigo 25, parágrafo terceiro, da Convenção prevê também uma forma célere e eficaz de auxílio entre os Estados:

> Em caso de urgência, cada Parte pode formular os pedidos de auxílio mútuo ou comunicações com ele relacionadas, através de meios de comunicação rápidos, tais como o fax ou o correio electrónico, desde que esses meios ofereçam condições de segurança e de autenticação (incluindo, se necessário, o uso da encriptação) com posterior confirmação oficial sempre que o Estado requerido o exigir. O Estado requerido aceitará o pedido e responderá através de qualquer desses meios de comunicação rápidos.[105]

Dessa forma, a cooperação se daria de forma muito mais rápida, garantindo que a investigação não sofra entraves e continue produzindo provas idoneamente, com segurança e sem ofender garantias e princípios mínimos.

Vale ressaltar que o Brasil ainda não aderiu à Convenção de Budapeste, embora tenha sido convidado. No entanto, em julho de 2020 foi enviado ao Congresso Nacional o texto da Convenção para que o Brasil adira ao instrumento[106]. Entretanto, isso não quer dizer que o país não venha desempenhando um papel importante na cooperação jurídica internacional, inclusive quanto aos crimes cibernéticos.

---

[105] BRASIL. Ministério Público Federal. **Convenção Sobre o Cibercrime.** Budapeste, 23 nov. 2001. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf. Acesso em: 29 ago. 2020.

[106] GOVERNO FEDERAL. **Brasil é convidado a aderir à Convenção do Conselho da Europa contra a Criminalidade Cibernética**: Convite para adesão vale por três anos e irá proporcionar maior cooperação jurídica internacional voltada aos crimes cibernéticos. Brasília, DF: Secretaria-Geral, 24 jul. 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#:~:text=Conven%C3%A7%C3%A3o%20contra%20a%20Criminalidade%20Cibern%C3%A9tica,o%20combate%20ao%20crime%20cibern%C3%A9tico. Acesso em: 23 mar. 2021.

4.3 O PAPEL DO BRASIL NA COOPERAÇÃO INTERNACIONAL E A NECESSIDADE DE HARMONIZAÇÃO COM A CONVENÇÃO DE BUDAPESTE

Nos últimos anos, o Brasil tem proporcionado uma maior participação com a comunidade internacional em termos de acordos em matéria penal, sujeitando-se à jurisdição de Cortes estrangeiras e também realizando acordos e protocolos de assistência mútua. Essa relação internacional está prevista inclusive na Constituição Federal, no seu art. 4º e incisos, conforme já visto anteriormente.

A Emenda Constitucional 45/2004 representa um marco nas relações internacionais ao introduzir o §3º do art. 5º, que elevou os tratados e convenções internacionais sobre direitos humanos à categoria de Emenda Constitucional, o que acabou por resolver o conflito entre a hierarquia de tratados internacionais dentro do ordenamento nacional. Prevê, assim, o referido parágrafo e artigo:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> (...)
> § 3º Os tratados e convenções internacionais sobre direitos humanos que forem aprovados, em cada Casa do Congresso Nacional, em dois turnos, por três quintos dos votos dos respectivos membros, serão equivalentes às emendas constitucionais.

Além disso, a Constituição Federal ainda estabelece a competência dos órgãos no que diz respeito aos procedimentos oriundos da cooperação jurídica internacional. O Supremo Tribunal Federal, por exemplo, é o órgão competente para processar o julgar pedidos de extradição solicitados por Estado estrangeiro, conforme art. 102, inciso I, alínea “g” da Carta Magna. O Superior Tribunal de Justiça detém a competência para homologação de sentenças estrangeiras e a concessão de exequatur às cartas rogatórias, conforme previsão do art. 105, inciso I, alínea “i”, da CF. Por fim, compete à Justiça Federal a execução de carta rogatória, após o exaquatur, e da sentença estrangeira após homologação, conforme art. 109, inciso X, da CF.

Por meio da legislação infraconstitucional, mormente o Código de Processo Penal, por meio do art. 780 e seguintes, tem-se o regramento das relações com

autoridades estrangeiras, especialmente quanto às cartas rogatórias e as homologações de sentenças estrangeiras.

Quanto às cartas rogatórias, que se trata do instrumento utilizado para comunicação entre autoridades nacionais e estrangeiras para a cooperação jurídica, o artigo 783 do CPP prevê a necessidade de sua remessa pelo juiz singular ao Ministro da Justiça, o qual dará cumprimento por via diplomática às autoridades estrangeiras competentes. Além da carta rogatória, existe ainda o auxílio direto, outro instrumento de cooperação jurídica internacional que se verá mais à frente e tem ajudado na celeridade e desburocratização da cooperação jurídica internacional.

Em que pese o Brasil tenha grandes vínculos diplomáticos com a maioria dos países do mundo, a quantidade de instrumentos assinados com outros Estados em matéria penal ainda é baixa. Segundo dados do Ministério da Justiça e Segurança Pública[107], o país possui 14 Convenções Internacionais de acordos multilaterais, ou seja, aqueles em que diversos países são assinantes, e apenas 21 acordos bilaterais, ou seja, aqueles em que apenas o Brasil e outro Estado são partes. Nenhum deles diz respeito exclusivamente aos crimes virtuais.

Por outro lado, nem toda cooperação precisa da intervenção do Poder Judiciário para sua validade e eficiência. É o caso da Cooperação Direta entre as Polícias, que ocorre pelo "intercâmbio de informações policiais através da Interpol"[108], em que a autoridade nacional busca a realização de uma diligencia investigativa no território de outro país, ou vice-versa.

Um exemplo da eficácia dessa cooperação é a troca de informações entre o Conselho de Controle de Atividades Financeiras (COAF) no Brasil, unidade de inteligência especializada na repressão e prevenção de crimes contra a ordem econômica do país, entre elas a lavagem de dinheiro e o financiamento do terrorismo[109], e as unidades de Inteligência financeira de outros países. Outro exemplo trazido por Alesandro Gonçalves Barreto e Beatriz Silveira Brasil[110] é o da

---

[107] MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. **Acordos Internacionais**. Brasília, DF: Ministério da Justiça e Segurança Pública, [20--]. Disponível em: https://legado.justica.gov.br/sua-protecao/cooperacao-internacional/cooperacao-juridica-internacional-em-materia-penal/acordos-internacionais. Acesso em: 15 abr. 2021.

[108] BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silvera. **Manual de Investigação Cibernética: à Luz do Marco Civil da Internet**. Rio de Janeiro: Editora Brasport, p. 52, 2016.

[109] COAF. **O que faz o COAF?** Brasília, DF: COAF, dez. 2020. Disponível em: https://www.gov.br/coaf/pt-br/centrais-de-conteudo/publicacoes/publicacoes-do-coaf-1/o-que-faz-o-coaf-versao-20200124.pdf/. Acesso em: 06 jun. 2021.

[110] Ibid.

Operação Tapete Persa, que se tratou de uma investigação envolvendo a Interpol, polícia federal brasileira e polícia alemã, para apurar crimes de abuso sexual e pedofilia na Internet. No caso, as investigações da polícia alemã identificaram IPs situados no Brasil de rede de compartilhamento de arquivos envolvendo pornografia infantil. Assim que recebida a informação pelo Brasil, instaurou-se os Inquéritos Policiais para apuração dos fatos, além de mandados de prisão e de busca e apreensão feitos em dez estados brasileiros[111].

Ressalta-se que essa cooperação é feita pela Polícia Federal dentro do território brasileiro, uma vez que é sua atribuição, conforme anteriormente citado, e a faz por meio da Coordenação-Geral de Cooperação Internacional (CGCI), parte do Departamento de Polícia Federal (DPF)[112]. Essa Coordenação-Geral se divide em três seções, sendo ela a de Setor de Apoio Administrativo (SAD), Setor de Apoio às Missões Exteriores (SEMEX), Serviço de Cooperação Policial (INTERPOL), e a Divisão de Cooperação Jurídica Internacional (DJC).

Dentre suas atribuições está o intercâmbio de informações com outras entidades de mesmo gênero e organizações reconhecidas pelo Brasil que congreguem organismos policiais e que possuam interesse na investigação de algum fato. São exemplos a Interpol, Europol, Ameripol, dentre outras instituições intergovernamentais.

Necessário apontar que essas instituições não possuem informações que interessam a investigação em andamento, ou seja, elas apenas auxiliam e atuam como órgãos intermediários, garantindo a efetiva e direta cooperação entre as policiais nacionais e internacionais. É o caso, por exemplo, do cumprimento de um mandado de prisão de um foragido, em que a Interpol auxilia a polícia local no cumprimento da ordem.

Dessa forma, apesar de o Brasil, nos últimos anos, ter caminhado no sentido de uma busca maior pela cooperação jurídica internacional, percebe-se que para o efetivo combate do crime cibernético, que não respeita fronteiras, é necessária uma

---

[111] BONIN, Robson. Operação Tapete Persa prende 20 por abuso sexual e pedofilia, diz PF. Polícia Federal encontrou material pornográfico em nove estados. Número de prisões de supostos pedófilos é recorde, diz delegado. **G1**. Brasília, DF, 27 jul. 2010. Disponível em: http://g1.globo.com/brasil/noticia/2010/07/operacao-tapete-persa-prende-20-por-abuso-sexual-e-pedofilia-diz-pf.html. Acesso em: 29 abr. 2021.

[112] BRASIL. **Portaria nº 2.877, de 30 de dezembro de 2011**. Aprova o Regimento Interno do Departamento de Polícia Federal. Brasília, DF: Ministério da Justiça e Segurança Pública. Disponível em: https://www.justica.gov.br/Acesso/anexos-institucional/ri-departamento-de-policia-federal-dpf.pdf. Acesso em: 29 abr. 2021.

maior aproximação do país com o restante da comunidade internacional, especialmente para melhor enfrentar os desafios do combate à criminalidade e desburocratizar a cooperação jurídica internacional, tarefa essa que já é um desafio até mesmo para países mais atuantes no cenário penal mundial. Por isso mesmo que a Convenção de Budapeste apresenta diretrizes que uniformizam a forma como os Estados tratam do assunto, o que é urgentemente necessário internalizar no Brasil.

Sem dúvida nenhuma a adesão do Brasil à Convenção de Budapeste traria enormes benefícios ao país. Como citado anteriormente, o Brasil possui uma carência de legislação sobre cibersegurança e crimes cibernéticos, aliados ainda a uma deficiência de estrutura para combatê-los.

O próprio MPF emitiu parecer[113] solicitando mais celeridade na adesão à Convenção, alertando que os delitos informáticos não têm tido seu combate de forma eficiente pela falta de capacitação e ausência de ferramentas jurídicas aptas a permitir a persecução penal, o que acarreta em um aumento de insegurança dos usuários brasileiros na internet e dificultando a prevenção de ataques e ocorrências.

Além disso, foi ressaltado no parecer o aumento exponencial do número de crimes cibernéticos, com migração de delitos comuns para o meio digital. Da mesma forma, a obtenção de provas digitais para comprovação da materialidade e autoria delitiva de diversos crimes, inclusive homicídios e corrupção, dependem, muitas vezes, de interceptações telemáticas e arquivos hospedados em “nuvem”, o que se tornou rotina dentre os operadores do direito.

Dessa forma, a adesão do Brasil à Convenção melhoraria sobremaneira o arcabouço legal do país, permitindo a aprovação de tipos penais específicos, preenchendo importantes lacunas da legislação brasileira que têm prejudicado a efetiva persecução dos crimes cibernéticos. Ademais, a harmonização da legislação nacional com a legislação internacional facilitará a cooperação jurídica internacional em investigações e extradição dos envolvidos.

Quanto à obtenção de provas, a Convenção possibilitará a cooperação do Brasil com todos os países signatários, inclusive aqueles com os quais não possui acordos bilaterais de cooperação em matéria penal. A proteção de dados também

---

[113] BRASIL. Ministério Público Federal. Procuradoria-Geral da República. **Ofício nº 736/2020, de 30 de julho de 2020**. Convenção sobre o Crime Cibernético. Brasília, DF: Ministério Público Federal, 2020. Disponível em: http://www.mpf.mp.br/pgr/documentos/Oficio736DaviAlcolumbre.pdf. Acesso em: 01 mai. 2021.

será favorecida, eis que a Convenção permite a capacitação e aprimoramento dos investigadores por meio da troca de experiências.

Assim, a adesão à Convenção de Budapeste representaria um grande avanço na repressão dos crimes cibernéticos, uma vez que proporciona diretrizes fundamentais e soluções para uma tão recente e complexa modalidade criminosa.

Aliado a isso, é de fundamental importância que o Brasil tenha uma participação mais ativa no que se refere a essa matéria da comunidade internacional. E essa parceria com outros países pode ser feita de diversas maneiras, como aquelas já citadas no trabalho: a adoção de tratados e acordos que visem uma homogeneização das legislações, na qual se adotará princípios e garantias básicas, facilitando a investigação e colheita de provas, e o contato direto entre as autoridades, o que desburocratiza, torna mais célere a judicialização e preserva evidências, como, por exemplo, a adoção da rede 24/7.

5 CONSIDERAÇÕES FINAIS

O trabalho teve como principal objetivo mostrar como a cooperação jurídica internacional e, especialmente, a Convenção de Budapeste, o mais importante tratado sobre cibercrime, são ferramentas essenciais na repressão dos crimes cibernéticos no Brasil. Em uma sociedade extremamente conectada, a ocorrência de ilícitos no meio digital cresce exponencialmente a cada dia, conforme o ser humano fica mais dependente da internet e de dispositivos eletrônicos, seja para o uso profissional ou pessoal. É quase impossível imaginar uma sociedade sem as facilidades que a internet e a tecnologia proporcionam.

Pode-se afirmar que o Brasil, apesar de seu esforço na criação de leis que auxiliem na segurança virtual de seus nacionais, como o Marco Civil da Internet, a Lei Geral de Proteção de dados e as novas leis que preveem as mais recorrentes condutas delitivas no ciberespaço, ainda assim, não dispõe de meios suficientes para coibir de forma eficaz a prática de crimes informáticos, por diversos fatores, como ausência de criminalização de alguns ataques cibernéticos considerados importantes, por carência da estrutura tecnológica da polícia judiciária para realizar investigações ou, ainda, pela morosidade da Justiça.

Assim, mesmo na perspectiva da política de controle, não basta uma legislação que incrimine determinadas condutas ilícitas, enquanto persiste uma série de entraves à persecução penal, como é o caso da adoção de teoria territorial incompatível com a modalidade de crime cibernético e a redação de normas que reproduzem interpretações dúbias, como o artigo 154-A do Código Penal, por exemplo.

Frisa-se, não há de se olvidar que o Direito Penal configura como *ultima ratio* no ordenamento jurídico e se está longe de querer transpassar um viés exclusivamente punitivista com o presente trabalho. Entretanto, também não se pode desconsiderar que muitas condutas criminosas no meio virtual ainda apresentam ameaças e não possuem tipificação, abrindo espaço para a impunidade dessas ações, e outras que sequer são conhecidas ainda, tendo em vista que em se tratando de tecnologia, informática e meio virtual, todos os dias se descobre novidades.

Nessa dimensão, em razão da natureza transacional do crime cibernético, a elaboração de legislação interna conectada ao direito penal e convenções internacionais com as finalidades da prevenção e persecução do crime tecnológico é de suma importância, como ponto de partida para o adequado tratamento e enfrentamento da criminalidade eletrônica.

É por meio da cooperação jurídica internacional que a imagem de facilidade em cometer crimes pela internet e permanecer impune é alterada. O Brasil já possui grandes relações diplomáticas com diversos países do globo, mas é apenas com a maior aproximação da comunidade internacional que o panorama dos crimes cibernéticos que ocorrem dentro do território é mudada.

Nesse feito, a Convenção de Budapeste representaria grande avanço e traria benefícios importantes dentro do ordenamento jurídico, devendo ser uma das urgências do Estado aderir ao tratado, possibilitando uma estreita conexão com Estados estrangeiros, mútua cooperação e desburocratização das investigações.

Destaca-se, ainda, os principais benefícios trazidos com a internalização da Convenção de Budapeste, como a Rede 24/7, a possibilidade de o Estado abdicar da sua prerrogativa de processamento e julgamento de nacional que cometeu crime no exterior, bem como termos técnicos universais, normas de direito material e o comprometimento do Brasil no engajamento da repressão dos delitos cibernéticos junto à comunidade internacional.

Aliado a tudo isso, o investimento em capacitação e estrutura tecnológica também representa grande parte no objetivo. Existem diversos instrumentos que podem ser usados para diminuir a incidência dos crimes cibernéticos, como, por exemplo, a criação de um grupo especializado em diversas áreas de conhecimento, para que possam analisar as qualidades e deficiências legislativas, propondo maneiras mais eficazes de assegurar a proteção do sistema e dos usuários; a promoção de cursos, em instituições educativas, enfatizando sobre os riscos existentes na internet e sobre posturas éticas que devem ser seguidas quando se está na rede; a instalação de medidas de segurança aos os usuários; a criação de agências especializadas na repressão dos crimes, dentre outras medidas.

O Brasil tem capacidade e disposição para reprimir a delinquência cibernética. Percebe-se, nos últimos anos, um grande avanço no arcabouço legislativo interno de preocupação com a segurança virtual, que tem aptidão de incorporar a Convenção de Budapeste em seu ordenamento, o que promoverá apenas benefícios ao país.

REFERÊNCIAS

ALECRIM, Emerson. Ataque hacker derruba sistemas do TJRS com ransomware: TJRS aparenta ter sido alvo de ransomware do grupo REvil, que teria pedido resgate de US$ 5 milhões. **Tecnoblog**, Brasil, 30 abr. 2021. Disponível em: https://tecnoblog.net/437846/ataque-hacker-derruba-sistemas-tjrs-ransomware/. Acesso em: 01 mai. 2021.

APPLE oferece US$ 1 milhão para quem hackear iPhone: O prêmio será concedido para pesquisadores e engenheiros de sistemas que encontram falhas no núcleo do sistema operacional iOS. **Época Negócios Online**, Rio de Janeiro, 12 de ago. de 2019. Disponível em: https://epocanegocios.globo.com/Empresa/noticia/2019/08/apple-oferece-us-1-milhao-para-quem-hackear-iphone.html. Acesso em: 26 ago. 2020.

ASSOCIAÇÃO PAULISTA DE MAGISTRADOS. **Enunciados do Fórum de Juizados Especiais do Estado de São Paulo (FOJESP)**: Minuta consolidada em 12/06/2018. São Paulo: APAMAGIS, 2018. Disponível em: https://apamagis.com.br/institucional/fojesp/. Acesso em: 29 mar. 2021.

BARATTA, Alessandro. **Criminologia Crítica e Crítica do Direito Penal**. 2 ed. Rio de Janeiro: Freitas Bastos, 1999.

BARRETO, Alesandro Gonçalves. **Análise da lei Azeredo:** necessidade de criação de delegacias e setores especializados na repreensão aos crimes informáticos. Brasil: Migalhas, 11 abr. 2018. Disponível em: https://migalhas.uol.com.br/depeso/278027/analise-da-lei-azeredo-necessidade-de-criacao-de-delegacias-e-setores-especializados-na-repreensao-aos-crimes-informaticos. Acesso em: 09 nov. 2020.

BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silvera. **Manual de Investigação Cibernética: à Luz do Marco Civil da Internet**. Rio de Janeiro: Editora Brasport, 2016.

BARRETO, Alessandro Gonçalves; KUFA, Karina; SILVA, Marcelo Mesquita. **Cibercrimes e Seus Reflexos no Direito Brasileiro**. Salvador: Editora Juspodivm, 2020.

BECHARA, Fábio Ramazzini; FLORES, Dímitri Molina. Crimes Cibernéticos: qual é o lugar do crime para fins de aplicação da pena e determinação da competência jurisdicional?. **Revista Direito Mackenzie**, São Paulo, v. 13, n. 2, 2019. Disponível em: http://editorarevistas.mackenzie.br/index.php/rmd/article/view/13357/10572. Acesso em: 17 set. 2020.

BITENCOURT, Cezar Roberto. **Código Penal Comentado**. 8. ed. São Paulo: Saraiva, 2014.

BONIN, Robson. Operação Tapete Persa prende 20 por abuso sexual e pedofilia, diz PF. Polícia Federal encontrou material pornográfico em nove estados. Número de

prisões de supostos pedófilos é recorde, diz delegado. **G1**. Brasília, DF, 27 jul. 2010. Disponível em: http://g1.globo.com/brasil/noticia/2010/07/operacao-tapete-persa-prende-20-por-abuso-sexual-e-pedofilia-diz-pf.html. Acesso em: 29 abr. 2021.

BOTELHO, Flávio. Não caia no golpe! Crimes cibernéticos aumentaram 347%: Governo lança cartilhas para te ajudar a evitar armadilhas no mundo virtual. **Agência Brasília**, Brasília, DF, 18 ago. de 2020. Disponível em**:** https://agenciabrasilia.df.gov.br/2020/08/17/nao-caia-no-golpe-crimes-ciberneticos-aumentaram-347/#:~:text=Entre%20janeiro%20e%20junho%20deste,mesmo%20per%C3%ADodo%20do%20ano%20passado.&text=Os%20meses%20de%20abril%20e,%3A%20624%20e%20708%2C%20respectivamente. Acesso em: 17 set. 2020.

BRASIL. Agência Nacional de Telecomunicações. **Norma nº 004/95**. Uso de Meios da Rede Pública de Telecomunicações para acesso à Internet. Aprovada pela Portaria nº 148/95. Brasília, DF: ANATEL, [1995]. Disponível em: https://www.anatel.gov.br/hotsites/Direito_Telecomunicacoes/TextoIntegral/ANE/prt/minicom_19950531_148.pdf. Acesso em: 27 abr. 2021.

BRASIL. **Decreto-lei nº 2.848, de 7 de dezembro de 1940.** Código Penal. Brasília, DF: Congresso Nacional [1940]. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 29 ago. 2020.

BRASIL. **Lei nº 9.099, de 26 de setembro de 1995.** Dispõe sobre os Juizados Especiais Cíveis e Criminais e dá outras providências. Brasília, DF: Congresso Nacional [1995]. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9099.htm. Acesso em: 29 mar. 2021.

BRASIL. **Lei nº 12.735, de 30 de novembro de 2012**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Brasília, DF: Congresso Nacional [2012]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 29 ago. 2020.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, DF: Congresso Nacional [2012]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 29 ago. 2020.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Congresso Nacional [2014]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 08 nov. 2020.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais e altera a lei nº 12965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Congresso Nacional [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 08 nov. 2020.

BRASIL. **Lei nº 14.155, de 27 de maio de 2021**. 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. Brasília, DF: Congresso Nacional [2021]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14155.htm. Acesso em: 29 mai. 2021.

BRASIL. Ministério da Justiça. **Cartilha de Cooperação Jurídica Internacional em Matéria Penal**. Brasília, DF: Ministério da Justiça, 2014. Disponível em: https://www.justica.gov.br/sua-protecao/lavagem-de-dinheiro/institucional-2/publicacoes/arquivos/cartilha-penal-09-10-14-1.pdf. Acesso em: 12 abr. 2021.

BRASIL. Ministério Público Federal. **Convenção Sobre o Cibercrime.** Budapeste, 23 nov. 2001. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf. Acesso em: 29 ago. 2020.

BRASIL. Ministério Público Federal. **Minuta do Relatório Explicativo**. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/coordenacao/comissoes-e-grupos-de-trabalho/combate-crimes-cirberneticos/convention-on-cybercrime/explanatory-reports_pt.pdf. Acesso em: 06 jun. 2021.

BRASIL. Ministério Público Federal. Procuradoria-Geral da República. **Ofício nº 736/2020, de 30 de julho de 2020**. Convenção sobre o Crime Cibernético. Brasília, DF: Ministério Público Federal, 2020. Disponível em: http://www.mpf.mp.br/pgr/documentos/Oficio736DaviAlcolumbre.pdf. Acesso em: 01 mai. 2021.

BRASIL. **Portaria nº 2.877, de 30 de dezembro de 2011**. Aprova o Regimento Interno do Departamento de Polícia Federal. Brasília, DF: Ministério da Justiça e Segurança Pública. Disponível em: https://www.justica.gov.br/Acesso/anexos-institucional/ri-departamento-de-policia-federal-dpf.pdf. Acesso em: 29 abr. 2021.

BRASIL. Senado Federal. **Projeto de Lei do Senado nº 236/2012.** Anteprojeto de Código Penal. Brasília, DF: Senador Federal [2012]. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=3515262&ts=1613697834640&disposition=inline. Acesso em: 26 mar. 2021.

BRASIL. Superior Tribunal de Justiça. **Conflito de Competência nº 107.938 - RS (2009/0183264-2).** Conflito de Competência. Processual Penal. Racismo praticado através de publicação de mensagens racistas em sítio de relacionamento. Internet.

Identificação dos autores. Necessidade. Local do crime. Lugar de onde foram enviados os textos ofensivos. Ausência de dados aptos a provar a origem das ofensas. Continuidade do procedimento investigatório. Prevenção. Competência daquele Juízo que primeiro conheceu da investigação. Suscitante: Juízo Federal da Vara Criminal e Juizado Especial Adjunto de Novo Hamburgo - SJ/RS. Suscitado: Juízo Federal da 4ª Vara Criminal da Seção Judiciária do Estado do Rio de Janeiro. Relator: Min. Jorge Mussi, 27 de outubro de 2010. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/17358831/conflito-de-competencia-cc-107938-rs-2009-0183264-2/inteiro-teor-17358832?ref=amp. Acesso em: 01 mai. 2021.

BRASIL. Superior Tribunal de Justiça. **Conflito de Competência nº 132.346 - RS (2014/0023833-8)**. Decisão Monocrática do Conflito de Competência. Suscitante: Juízo Federal da 11ª Vara da Seção Judiciária do Estado do Rio Grande do Sul. Suscitado: Juízo Federal da 3ª Vara da Seção Judiciária do Estado da Paraíba; Juízo Federal da 4ª Vara da Seção Judiciária do Estado do Rio de Janeiro. Relator: Min. Rogerio Schietti Cruz, 05 de agosto de 2015. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/893093395/conflito-de-competencia-cc-132346-rs-2014-0023833-8/decisao-monocratica-893093455?ref=juris-tabs. Acesso em: 01 mai. 2021.

BRASIL. Superior Tribunal de Justiça (6. Turma). **Habeas Corpus nº 41.348 - SP**. Penal e Processual. Habeas Corpus substitutivo de Recurso Ordinário. Crime de Usura. Inquérito Policial. Ausência de Justa Causa. Lei 9.000/95. Possibilidade de instauração de inquérito Policial. Denegação da Ordem. Relator: Min. Hélio Quaglia Barbosa, 02 de agosto de 2005. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/1805102/habeas-corpus-hc-41348-sp-2005-0013966-9/inteiro-teor-12957410. Acesso em: 29 mar. 2021.

BRASIL. Superior Tribunal de Justiça (3. Turma). **Recurso Especial Nº 1.745.657 – SP (2018/0062504-5)**. Recurso Especial. Internet. Jurisdição. Soberania Digital. Prequestionamento. Ausência. Marco Civil da Internet. Alcance. Aplicação da Legislação Brasileira. Pertinência da Jurisdição Nacional. Recorrente: Microsoft Informática LTDA. Recorrido: Luis Agostinho Marques Caso Quintiliano; Tam Linhas Aéreas S/A. Relatora: Min. Nancy Andrighi, 03 de novembro de 2020. Disponível em: https://arquivos-trilhante-sp.s3.sa-east-1.amazonaws.com/documentos/informativos-julgados/ffc43ebc9da5bdb81c0b518e9ba925f1.pdf. Acesso em: 01 mai. 2021.

BRASIL. Superior Tribunal de Justiça (5. Turma). **Recurso em Habeas Corpus nº 95.784 - PR**. Recurso Ordinário de Habeas Corpus. Tráfico e associação para o tráfico de entorpecentes e porte ilegal de arma de fogo de uso permitido. Negativa de autoria e inexistência de prova de materialidade [...]. Recorrente: Priscila Santos de Castro (preso). Recorrido: Ministério Público do Estado do Paraná. Relator: Min. Joel Ilan Paciornik, 06 de dezembro de 2018. Disponível em: https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1780840&num_registro=201800552717&data=20181219&peticao_numero=-1&formato=PDF. Acesso em: 01 mai. 2021.

BRASIL. Supremo Tribunal Federal (2. Turma). **Questão de Ordem na Prisão Preventiva para Extradição 732.** Extradição. Prisão Cautelar. Pleito formulado pela

Interpol. Possibilidade. Inovação introduzida pela lei nº 12.878/2013. Delito Informático (crime digital): “Invasão de dispositivo informático”. Relator: Min. Celso de Mello, 11 de novembro de 2014. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=7645112. Acesso em: 12 abr. 2021.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 628.624/MG.** Recurso Extraordinário. Repercussão Geral Reconhecida. Penal. Processo Penal. Crime previsto no artigo 241ª da Lei 8.069/90 (Estatuto da Criança e do Adolescente). Competência. Divulgação e publicação de imagens com conteúdo pornográfico envolvendo criança ou adolescente. Convenção sobre direitos da criança. Delito cometido por meio da rede mundial de computadores (Internet). Internacionalidade. Artigo 109, V, da Constituição Federal. Competência da Justiça Federal reconhecida. Recurso Desprovido. Recorrente: Fábio. Recorrido: Ministério Público Federal. Relator: Min. Marco Aurélio, 29 de outubro de 2015. Disponível em: https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=10667081. Acesso em: 01 mai. 2021

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário nº 778.054.** Agravo. Recorrente: Cooperativa Regional dos Produtores de Açúcar e Álcool de Alagoas. Recorrido: Banco Econômico SA. Relatora: Min. Cármen Lúcia, 23 de outubro de 2013. Disponível em: http://www.stf.jus.br/portal/processo/verProcessoPeca.asp?id=181471055&tipoApp=.pdf. Acesso em: 01 mai. 2021.

CAPEZ, Fernando; PRADO, Stela. **Código Penal Comentado**. 5. ed. São Paulo: Saraiva, 2014.

CAROLINA Dieckmann fala pela 1ª vez sobre fotos e diz que espera 'justiça': Atriz deu entrevista a Patricia Poeta no Jornal Nacional desta segunda (14). Trinta e seis fotos pessoais dela foram publicadas na internet. **G1,** São Paulo, 15 mai. 2012. Disponível em: http://g1.globo.com/pop-arte/noticia/2012/05/carolina-dieckmann-fala-pela-1-vez-sobre-roubo-de-fotos-intimas.html. Acesso em: 05 abr. 2021.

CARONE, Carlos. Estelionato na internet cresceu mais de 1.200% no DF durante pandemia: Metrópoles teve acesso a mapeamento dos crimes em todas as regiões do DF. De fraude a pedofilia, veja os cibercrimes que mais têm aumentado. **Metrópoles,** Brasília, DF, 12 abr. 2021. Disponível em: https://www.metropoles.com/distrito-federal/estelionato-na-internet-cresceu-mais-de-1-200-no-df-durante-pandemia. Acesso em: 01 mai. 2021.

CASELLI. Guilherme, BARRETO. Alessandro Gonçalves, GAUDENCIO, Andressa. Aplicação de modernas técnicas de investigação digital pela Polícia Judiciária e sua efetividade. **Direito & TI**, Brasil, 01 mai. 2016. Disponível em: http://direitoeti.com.br/artigos/aplicacao-de-modernas-tecnicas-de-investigacao-digital-pela-policia-judiciaria-e-sua-efetividade**/**. Acesso em: 16 set. 2020.

CENTRO REGIONAL DE ESTUDOS PARA O DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO. **TIC Domicílios:** Pesquisa sobre o Uso das Tecnologias de Informação e Comunicação nos Domicílios Brasileiros 2018. São

Paulo: Comitê Gestor da Internet no Brasil, 2019. Disponível em: https://cetic.br/media/docs/publicacoes/2/12225320191028-tic_dom_2018_livro_eletronico.pdf. Acesso em: 23 ago. 2020.

CERQUEIRA, Silvio Casto. ROCHA, Claudionor. Crimes Cibernéticos: desafios da investigação. **Cadernos ASLEGIS,** Brasília, DF, n. 49, mai./ago. 2013. Disponível em: https://www.google.com/url?q=https://www.aslegis.org.br/todas-as-edicoes-artigos/655-cadernos-aslegis-49&sa=D&source=editors&ust=1623087800217000&usg=AOvVaw1NF1RgsfdQyoj2HvmbltSh. Acesso em: 29 ago. 2020.

COAF. **O que faz o COAF?** Brasília, DF: COAF, dez. 2020. Disponível em: https://www.gov.br/coaf/pt-br/centrais-de-conteudo/publicacoes/publicacoes-do-coaf-1/o-que-faz-o-coaf-versao-20200124.pdf/. Acesso em: 06 jun. 2021.

CONSELHO EUROPEU. **O novo Centro Europeu de Competências em Cibersegurança ficará instalado em Bucareste, na Roménia**. Bruxelas: Conselho Europeu, 10 dez. 2020. Disponível em: https://www.consilium.europa.eu/pt/press/press-releases/2020/12/10/the-new-european-cybersecurity-competence-centre-to-be-located-in-bucharest-romania/#:~:text=O%20Centro%20de%20Compet%C3%AAncias%20em,industrial%20na%20%C3%A1rea%20da%20ciberseguran%C3%A7a. Acesso em: 13 abr. 2021.

CONSELHO EUROPEU. **Cibersegurança:** como combate a UE as ciberameaças. Bruxelas: Conselho Europeu, 21 abr. 2021. Disponível em: https://www.consilium.europa.eu/pt/policies/cybersecurity/. Acesso em: 13 abr. 2021.

CONSELHO NACIONAL DE JUSTIÇA. **Enunciados Cíveis**. Brasília, DF: CNJ, [20--]. Disponível em: https://www.cnj.jus.br/corregedoria-nacional-de-justica/redescobrindo-os-juizados-especiais/enunciados-fonaje/enunciados-civeis/. Acesso em: 29 mar. 2021.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 5. ed. São Paulo: Saraiva, 2010.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011.

CUNHA, Rogério Sanches, **Manual de Direito Penal:** Parte Especial (arts. 121 ao 361). 11. ed. Salvador: JusPODIVM, 2019.

DENÚNCIAS de crimes cometidos pela internet mais que dobram em 2020: Foram 156.692 notificações anônimas de janeiro a dezembro do ano passado, contra 75.428 em 2019. Ocorrências foram lideradas, mais uma vez, pela pornografia infantil, com quase 100 mil acusações. **G1,** Brasil, 09 fev. 2021. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/02/09/numero-de-denuncias-de-crimes-cometidos-pela-internet-mais-que-dobra-em-2020.ghtml. Acesso em: 01 mai. 2021.

DISTRITO FEDERAL. Tribunal de Justiça do Distrito Federal e Territórios (1. Turma). **Acórdão nº 824.525**, Apelação Cível do Juizado Especial. Processo nº

20130111169797ACJ. [...] A mera juntada da foto da tela do computador (print screen), cuja informação é produzida unilateralmente e sem o crivo do contraditório e da ampla defesa, não atende os ditames da lei processual, de modo a amparar qualquer juízo de valor negativo à pretensão do autor [...]. Relator: Juiz Luís Gustavo B. De Oliveira, 23 de setembro de 2014. Disponível em: https://pesquisajuris.tjdft.jus.br/IndexadorAcordaos-web/sistj?visaoId=tjdf.sistj.acordaoeletronico.buscaindexada.apresentacao.VisaoBuscaAcordao&nomeDaPagina=buscaLivre2&buscaPorQuery=1&baseSelecionada=TURMAS_RECURSAIS&filtroAcordaosPublicos=false&camposSelecionados=[ESPELHO]&argumentoDePesquisa=&numero=824525&tipoDeRelator=TODOS&dataFim=&indexacao=&ramoJuridico=&baseDados=[TURMAS_RECURSAIS,%20BASE_ACORDAOS_IDR,%20BASE_TEMAS,%20BASE_ACORDAOS,%20BASE_INFORMATIVOS]&tipoDeNumero=NumAcordao&tipoDeData=DataPublicacao&ementa=&filtroSegredoDeJustica=false&desembargador=&dataInicio=&legislacao=&orgaoJulgador=&numeroDaPaginaAtual=1&quantidadeDeRegistros=20&totalHits=1. Acesso em: 01 mai. 2021.

DISTRITO FEDERAL. Tribunal de Justiça do Distrito Federal e Territórios (5. Turma). **Acórdão nº 1019661.** Apelação Cível. Processo 20150110697772APC. [...] 5 - O print screen das telas do sistema da ré não é apto a comprovar a legitimidade das faturas, haja vista ser documento produzido unilateralmente, cujos dados foram inseridos pelos prepostos da ré sem qualquer possibilidade do consumidor ter conhecimento deles [...]. Relatora: Maria Ivatônia, 24 de maio de 2017. Disponível em: https://pesquisajuris.tjdft.jus.br/IndexadorAcordaos-web/sistj?visaoId=tjdf.sistj.acordaoeletronico.buscaindexada.apresentacao.VisaoBuscaAcordao&nomeDaPagina=buscaLivre2&buscaPorQuery=1&baseSelecionada=BASE_ACORDAOS&filtroAcordaosPublicos=false&camposSelecionados=[ESPELHO]&argumentoDePesquisa=&numero=1019661&tipoDeRelator=TODOS&dataFim=&indexacao=&ramoJuridico=&baseDados=[TURMAS_RECURSAIS,%20BASE_ACORDAOS_IDR,%20BASE_TEMAS,%20BASE_ACORDAOS,%20BASE_INFORMATIVOS]&tipoDeNumero=NumAcordao&tipoDeData=DataPublicacao&ementa=&filtroSegredoDeJustica=false&desembargador=&dataInicio=&legislacao=&orgaoJulgador=&numeroDaPaginaAtual=1&quantidadeDeRegistros=20&totalHits=1. Acesso em: 01 mai. 2021.

EUROPOL. **About Europol.** Haia: Europol, [20--]. Disponível em: https://www.europol.europa.eu/about-europol. Acesso em: 06 jun. 2021.

FILHO, Demócrito Reinaldo. Limites e requisitos da ordem judicial para quebra de sigilo de dados armazenados por provedor de serviços na internet: Desnecessidade de individualização prévia do(s) investigado(s) e do esgotamento de outros meios de prova. **Jus,** Teresina, mar. 2020. Disponível em: https://jus.com.br/artigos/80222/limites-e-requisitos-da-ordem-judicial-para-quebra-de-sigilo-de-dados-armazenados-por-provedor-de-servicos-na-internet/3. Acesso em: 29 mai. 2021.

GOODMAN, Marc. **Future Crimes:** tudo está conectado, todos somos vulneráveis e o que podemos fazer sobre isso. Rio de Janeiro: Editora Alta Books, 2018.

GOVERNO FEDERAL. **Brasil é convidado a aderir à Convenção do Conselho da Europa contra a Criminalidade Cibernética**: Convite para adesão vale por três anos e irá proporcionar maior cooperação jurídica internacional voltada aos crimes cibernéticos. Brasília, DF: Secretaria-Geral, 24 jul. 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#:~:text=Conven%C3%A7%C3%A3o%20contra%20a%20Criminalidade%20Cibern%C3%A9tica,o%20combate%20ao%20crime%20cibern%C3%A9tico. Acesso em: 23 mar. 2021.

GOVERNO FEDERAL. Conselho de Controle de Atividades Financeiras. **Grupo de Ação Financeira contra a Lavagem de Dinheiro e o Financiamento do Terrorismo (Gafi/FATF)**. Brasília, DF: Governo Federal [20--]. Disponível em: https://www.gov.br/coaf/pt-br/atuacao-internacional/prevencao-e-combate-a-lavagem-de-dinheiro-e-ao-financiamento-do-terrorismo/gafi. Acesso em: 06 jun. 2021.

GOVERNO FEDERAL. Ministério das Relações Exteriores. **Notas à Imprensa nº 309/2019:** Processo de adesão à Convenção de Budapeste - Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública. Brasília, DF: Ministério das Relações Exteriores, 11 dez. 2019. Disponível em: https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/2019/processo-de-adesao-a-convencao-de-budapeste-nota-conjunta-do-ministerio-das-relacoes-exteriores-e-do-ministerio-da-justica-e-seguranca-publica. Acesso em: 29 ago. 2020.

GRECO, Rogério. **Código Penal Comentado**. 8. ed. Niterói: Impetus, 2014.

HAUTSCH, Oliver. O que é en genharia reversa? **Tecmundo**, [*s.l.*], 28 set. 2009. Disponível em: https://www.tecmundo.com.br/pirataria/2808-o-que-e-engenharia-reversa-.htm. Acesso em: 06 jun. 2021.

HTTRACK WEBSITE COPIER. **Free Software offline browser.** Disponível em: https://www.httrack.com/page/1/en/index.html. Acesso em: 09 nov. 2020.

INTERPOL. **What is INTERPOL?** Lion: INTERPOL, [20--]. Disponível em: https://www.interpol.int/Who-we-are/What-is-INTERPOL. Acesso em: 06 jun. 2021.

JESUS, Damásio de; MILAGRE, José Antonio. **Manual de Crimes Informáticos**. São Paulo: Saraiva, 2017.

KETHINENI, Sesha; CAO, Ying. The Rise in Popularity of Cryptocurrency and Associated Criminal Activity. **Sage Journals**, v. 30, n. 3, set. 2020. DOI: https://doi.org/10.1177/1057567719827051. Disponível em: https://journals.sagepub.com/doi/abs/10.1177/1057567719827051. Acesso em: 13 abr. 2021.

KUNRATH, Josefa Cristina Tomaz Martins. **A expansão da criminalidade no ciberespaço:** desafios de uma política criminal de prevenção ao cibercrime. 158 f. il.

2014. Dissertação (Mestrado) — Faculdade de Direito, Universidade Federal da Bahia, Salvador, 2014.

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. **Acordos Internacionais**. Brasília, DF: Ministério da Justiça e Segurança Pública, [20--]. Disponível em: https://legado.justica.gov.br/sua-protecao/cooperacao-internacional/cooperacao-juridica-internacional-em-materia-penal/acordos-internacionais. Acesso em: 15 abr. 2021.

NUCCI, Guilherme de Souza. **Código Penal Comentado**. 14. ed. Rio de Janeiro: Forense, 2014.

OLIVEIRA, Regiane; ROSSI, Marina. No submundo da internet, prospera o lucrativo negócio de chantagear empresas em meio à pandemia. **El País Brasil**, São Paulo, 03 jul. 2020. Disponível em: https://brasil.elpais.com/tecnologia/2020-07-03/no-submundo-da-internet-prospera-o-lucrativo-negocio-de-chantagear-empresas-em-meio-a-pandemia.html. Acesso em: 01 mai. 2021.

PARANÁ. Tribunal de Justiça do Paraná. **Conflito de Competência Crime nº 1.392.910-3.** Relator Convidado: Benjamim Acácio de Moura e Costa, 06 de novembro de 2015. Disponível em: https://tj-pr.jusbrasil.com.br/jurisprudencia/255319428/conflito-de-jurisdicao-cj-13929103-pr-1392910-3-decisao-monocratica/inteiro-teor-255319444. Acesso em: 29 mar. 2021.

PESQUISA NACIONAL POR AMOSTRA DE DOMICÍLIOS CONTÍNUA. **Acesso à Internet e à televisão e posse de telefone móvel celular para uso pessoal 2017**. Brasília, DF: PNAD contínua, [2018]. Disponível em: https://biblioteca.ibge.gov.br/visualizacao/livros/liv101631_informativo.pdf. Acesso em: 23 ago. 2020.

PETRY, Guilherme. Blockchain do crime: como investigar crimes com criptomoedas. **The Hack,** [*s.l.*], dez. 2020. Disponível em: https://thehack.com.br/blockchain-do-crime-como-investigar-crimes-com-criptomoedas/. Acesso em: 29 mai. 2021.

PINHEIRO, Patrícia Peck; HAIKAL, Victor Auilo. A nova lei de crimes digitais. **Gazeta do Povo**, [*s.l.*], 11 abr. 2013. Disponível em: https://www.gazetadopovo.com.br/vida-publica/justica-direito/artigos/a-nova-lei-de-crimes-digitais-evf935c0vqjw7rh9b4cq75tfy. Acesso em: 05 abr. 2021.

RIO GRANDE DO SUL. Tribunal de Justiça do Estado do Rio Grande do Sul. **Cartilha dos Juizados Especiais Cíveis**. Porto Alegre: Tribunal da Justiça, [20--]. Disponível em: https://www.tjrs.jus.br/novo/institucional/1o-grau/juizados-especiais/cartilha-dos-juizados-especiais/. Acesso em: 29 mar. 2021.

ROSA, Vitor. Investigações estão prejudicadas de maneira quase irreversível, diz chefe do MP sobre ataque hacker ao TJRS: Procurador Fabiano Dallazen se refere aos atrasos que serão gerados em escala e, também, ao temor do vazamento de dados. **GZH,** Porto Alegre, 30 abr. 2021. Disponível em: https://gauchazh.clicrbs.com.br/geral/noticia/2021/04/investigacoes-estao-

prejudicadas-de-maneira-quase-irreversivel-diz-chefe-do-mp-sobre-ataque-hacker-ao-tjrs-cko4s4pc400be018mrlsoeq90.html. Acesso em: 01 mai. 2021.

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004.

SÃO PAULO (Estado). Ministério Público do Estado de São Paulo. Centro de Apoio Operacional Criminal. **Nova lei de crimes cibernéticos entra em vigor.** São Paulo: MPSP, [2013].
Disponível em: http://www.mpsp.mp.br/portal/page/portal/cao_criminal/notas_tecnicas/NOVA%20LEI%20DE%20CRIMES%20CIBERN%C3%89TICOS%20ENTRA%20EM%20VIGOR.pdf. Acesso em: 05 abr. 2021.

SERGIPE. Tribunal de Justiça do Estado de Sergipe. **Acórdão nº 201818567**. Mandado de Segurança Cível. Processo 201800111901. Constitucional e Processo Penal. Mandado de Segurança. Inquérito policial. Investigação do homicídio do Comandante da Companhia Independente de Operações Policiais Especiais em área de Caatinga (CIOPAC). Decisão que determina a quebra de sigilo telemático [...]. Impenetrante: Google Brasil Internet LTDA; Google LLC; Impetrado: Juízo de Direito da Comarca de Porto da Folha. Relatora: Des. Iolanda Santos Guimarães, 22 de agosto de 2018. Disponível em: https://www.conjur.com.br/dl/tj-quebra-sigilo-generica-baseada-tempo.pdf. Acesso em: 20 abr. 2021.

SIGNIFICADOS BR. **Significado de Cyber**. Brasil, [20--]. Disponível em: https://www.significadosbr.com.br/cyber. Acesso em: 29 ago. 2020.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Jurisprudência do STJ:** Pesquisa de Jurisprudência. Brasília, DF, [2021]. Disponível em: https://scon.stj.jus.br/SCON/. Acesso em: 01 mai. 2021.

TOFFOLI, José Antonio Dias; CESTARI, Virgínia Charpinel Junger. Mecanismos de Cooperação Jurídica Internacional no Brasil. *In*: BRASIL. Ministério da Justiça. **Manual de Cooperação Jurídica Internacional e Recuperação de Ativos**: Cooperação em Matéria Civil. Brasília, DF: Ministério da Justiça, 2008. Disponível em: https://www.tjdft.jus.br/publicacoes/edicoes/manuais/manuais-da-corregedoria/2009Manual_CooperacaoCivil.pdf. Acesso em: 12 abr. 2021.

TRIBUNAL DE JUSTIÇA DO DISTRITO FEDERAL. **SISTJWEB:** Pesquisa Documentos Jurídicos. Disponível em: https://pesquisajuris.tjdft.jus.br/IndexadorAcordaos-web/sistj?visaoId=tjdf.sistj.acordaoeletronico.buscaindexada.apresentacao.VisaoBuscaAcordao. Acesso em: 09 nov. 2020.