A INVESTIGAÇÃO DE CRIMES PRATICADOS EM AMBIENTE VIRTUAL: ANÁLISE LEGAL E LIMITES INVESTIGATÓRIOS DA AUTORIA DELITIVA ESTRANGEIRA COM REFLEXOS DO DELITO NO BRASIL

CYBER CRIMES INVESTIGATION: LEGAL ANALYSIS AND INVESTIGATORY LIMITS OF THE FOREIGN CRIME AUTHORSHIP AND ITS REFLECTIONS IN BRAZIL

Luiz Felipe Valles Rosado[1]
Rodrigo Bueno Gusso[2]

Resumo: O presente estudo versa sobre os limites da investigação de crimes praticados em ambiente virtual, nos casos em que o autor está situado em país estrangeiro. A crescente utilização da *Internet* e as diversas plataformas virtuais auxiliam sobremaneira a vida em sociedade. Entretanto, é cediço que houve um grande incremento de delitos praticados valendo-se da rede mundial de computadores. Neste texto serão analisados os dispositivos legais pátrios acerca do tema, bem como as imperfeições legislativas e, em seguida, será apresentado um breve panorama a respeito de como alguns países têm lidado com os crimes virtuais. Os limites investigatórios da persecução criminal serão abordados, quando será discorrido acerca das alternativas de identificação e de responsabilização extraterritorial, bem como sobre a eficácia de tais meios para os inquéritos policiais nacionais, quando o autor do fato tenha praticado o delito fora do território brasileiro.

Palavras-chave: Investigação cibernética; *Internet*; autoria estrangeira.

Abstract: This article presents the limits of cyber crimes when the author is located in a foreign country. The growing use of the Internet and the various virtual platforms greatly help life in society. However, it is known that there has been a significant increase of crimes committed using the world wide web. In this text, the country's legal regulations about the subject will be analyzed, as well as the legislative imperfections, and then a brief overview will be presented about how some countries have dealt with virtual crimes. The investigative limits of criminal prosecution will be analyzed when the alternatives for identification and extraterritorial accountability are discussed, as well as the effectiveness of these means for national police investigations when the perpetrator has committed the crime outside Brazilian territory.

Keywords: Cyber Investigation; Internet; foreign authorship.

1 INTRODUÇÃO

A crescente utilização da *Internet* como facilitadora de comunicações e aquisições de produtos e serviços tem facilitado a vida em sociedade. Entretanto, ao passo em que a convivência social torna-se cada dia mais dependente da tecnologia direcionada à rapidez da vida moderna e da quebra de fronteiras, passa-se a viver em um ambiente predominantemente desconhecido, onde milhares de dados são inseridos diariamente.

Esse ambiente se torna amplamente favorável à prática criminosa, pois a "dependência" da rede mundial de computadores para tarefas básicas deixa lacunas abertas à invasão da privacidade em sentido amplo. Os criminosos virtuais, aproveitando-se, sobretudo,

[1]Delegado de Polícia Civil no Estado de Santa Catarina. Graduado em Direito pela UNIVALI, especialista em Gestão de Segurança Pública pela UNISUL e especialista em Gestão de Segurança Pública e Investigação Criminal Aplicada pela ACADEPOL – SC. Email: delrosado@gmail.com.
[2]Bacharel em Direito, especialista em Segurança Pública, mestre em Direito, doutor em Sociologia. Pesquisador do Centro de Estudos em Segurança Pública e Direitos Humanos (CESPDH) da Universidade Federal do Paraná (UFPR). Pós-Doutor em Democracia e Direitos Humanos pela Universidade de Coimbra, Portugal. Email: gusso@gusso.com.br.

do pseudoanonimato, buscam na rede satisfazer seu desejo ilícito a partir da vulnerabilidade dos usuários, uma vez que a *Internet* é utilizada por pessoas das mais variadas faixas etárias e de conhecimento.

Nesse cenário, em que há criminosos com conhecimentos e experiências diárias, tem-se, também, usuários de todos os tipos e perfis, formando um ambiente propício à prática de transgressões virtuais. Uma vez ocorrido o eventual crime, cabe à Polícia Civil a investigação do fato, no intuito de determinar as circunstâncias, a autoria etc. Contudo, a investigação dessa espécie de delito afigura-se como bastante complexa, pois é notória a disponibilidade de diversas ferramentas tecnológicas que o autor utiliza para se eximir de responsabilidades.

Para agravar esse fato, há os crimes virtuais praticados por autores que se encontram fora do território nacional, o que torna muito mais intricada a identificação e a responsabilização em virtude da soberania de cada país. Nesse sentido, o objetivo deste estudo foi analisar os problemas enfrentados pela Polícia Civil relacionados à investigação dos crimes virtuais, especialmente quando o autor pratica o ato fora do território nacional e as consequências recaem sobre vítimas brasileiras.

Na primeira seção do artigo será analisado o arcabouço jurídico pátrio a respeito dos crimes praticados em ambiente virtual. A comparação da legislação brasileira com a legislação estrangeira será apresentada a partir da segunda seção. Na terceira e última seção, o estudo restringir-se-á à análise dos crimes praticados em ambiente virtual ocorridos no Estado de Santa Catarina e investigados pela Polícia Civil.

No trabalho foram utilizadas fontes bibliográficas a fim de examinar os atuais problemas relacionados à cibercriminalidade mundial, bem como analisar documentos oficiais internacionais formalizados para a repressão a esse tipo de crime.

No Sistema Integrado de Segurança Pública (SISP), que é a ferramenta utilizada pela Polícia Civil do Estado de Santa Catarina para a formalização de Boletins de Ocorrência, foram consultados dados que denotam uma evolução dos crimes cibernéticos nos últimos anos. Destarte, o estudo pretendeu identificar os problemas relacionados com a criminalidade virtual procedente de país estrangeiro e propor soluções visando à repressão qualificada desses crimes.

2 A LEGISLAÇÃO BRASILEIRA ACERCA DOS CRIMES PRATICADOS EM AMBIENTE VIRTUAL

O Código Penal Brasileiro (Decreto-Lei n.º 2.848) é de 7 de dezembro de 1940. Inegavelmente, os padrões de convivência e costumes da sociedade de então eram bem diversos dos atuais. Ainda que múltiplas alterações tenham sido efetuadas durante esses anos de vigência do Código Penal Brasileiro, o legislador não vem conseguindo acompanhar a

rapidez que vem marcando o surgimento e as transformações dos crimes virtuais na contemporaneidade.

Para melhor entendimento dessa informação, é preciso esclarecer que a doutrina classifica os crimes virtuais em três modalidades. De acordo com Damásio Evangelista de Jesus (*apud* CARNEIRO, 2012), os crimes podem ser próprios, quando a conduta ilícita visa exclusivamente o sistema computacional; impróprios, quando a *Internet* é utilizada apenas como meio para a prática do delito; e, por fim, mistos, quando a *Internet* é condição indispensável para a ilegalidade, embora o bem jurídico visado pelo agente seja diverso do informático.

Tal classificação é importante a fim de demonstrar como o Código Penal regulamenta certas condutas ilícitas, pois aos crimes impróprios e mistos algumas figuras penais se amoldariam aos atos praticados. Entretanto, há certo descompasso no que tange aos delitos virtuais próprios, pois poucas condutas encontram-se tipificadas.

Nesse sentido, no ano de 2000, a Lei n.º 9.983 inseriu ao Código Penal, no Título XI – Dos Crimes conta a Administração Pública, os seguintes delitos:

> Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano:
> Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa.
> Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente:
> Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa.

Apenas doze anos depois dessa alteração legislativa, houve nova criminalização dos delitos praticados em ambiente virtual, com o surgimento das Leis n.º 12.735/2012 e 12.737/2012.

A Lei n.º 12.735/2012, que alterou o Código Penal, o Código Penal Militar, bem como a Lei n.º 7.716/89, após sofrer vetos nos artigos 2º e 3º, assim disciplinou em seu artigo 4º: “Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado” (BRASIL, 1989).

A referida norma ainda inseriu o inciso III ao parágrafo 3º do artigo 20, da Lei 7.716/89, que disciplina os crimes resultantes de preconceito de raça ou de cor, permitindo ao juiz que interdite mensagens ou páginas de informação na rede mundial de computadores que estejam violando o bem jurídico protegido.

A Lei n.º 12.737/2012 inseriu ao Código Penal os artigos 154-A, 154-B, os parágrafos 1º e 2º ao artigo 266 e o parágrafo único ao artigo 298. Essa lei ganhou grande apelo popular

a partir do caso envolvendo a atriz Carolina Dickmann (FMP, 2021) que foi vítima de *phishing*[3], quando seus arquivos pessoais foram divulgados pela *Internet* e determinados indivíduos passaram a exigir valores em troca dos arquivos subtraídos.

O tipo descrito no artigo 154-A[4] do Código Penal supriu a lacuna legislativa referente à invasão de dispositivo informático. Contudo, não chega a ser exaustivo e sofre críticas no que tange às brandas penas impostas, bem como à complexidade da investigação que demandaria a instauração de inquérito policial (NOGUEIRA, 2016, p. 27). Quanto ao artigo 154-B, do Código Penal, inserido pela Lei n.º 12.737/2012, trata-se de norma processual penal que define o tipo da ação penal em determinados casos.

Ainda com relação às inovações legislativas advindas da Lei n.º 12.737/12, houve mudança de nomenclatura do tipo descrito no artigo 266 do Código Penal para considerar como serviços de utilidade pública os meios informáticos e telemáticos. Por fim, a última mudança ocorreu com relação ao artigo 298, parágrafo único do Código Penal, que equiparou os cartões de crédito e de débito a documento particular.

Outras seis normas do Código Penal foram modificadas pela Lei n.º 13.718, de 24 de setembro de 2018 (BRASIL, 2018). Em todas elas há menção ao meio informático como causa de aumento de pena. Ao que interessa ao presente estudo, apenas o artigo 218-C, do Código Penal, foi analisado. Tal norma visou reprimir diversas formas de divulgação de conteúdo pornográfico adulto, consentido ou não, e, entre elas, incluiu o sistema de informática ou telemática.

Oportuno ressaltar que as legislações antes mencionadas também obtiveram intenso apelo popular, pois a inserção dos artigos 215-A e 218-C ao Código Penal advieram de fatos

---

[3] *Phishing* refere-se a uma maneira ilícita que cibercriminosos usam para persuadir alguém a revelar informações pessoais, como senhas ou cartão de crédito, CPF e número de contas bancárias. Eles fazem isso enviando emails falsos ou direcionando a pessoa a *websites* falsos. Disponível em: <https://www.avast.com/pt-br/c-phishing>. Acesso em: 24 jun. 2022.

[4] Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança, 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.
§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
§ 2o Aumenta-se a pena de um sexto a um terço 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 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
§ 4º Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
§ 5o Aumenta-se a pena de um terço à metade se o crime for praticado contra: I - Presidente da República, governadores e prefeitos; II - Presidente do Supremo Tribunal Federal; III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. Disponível em < http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm> Acesso em 24 jun. 2022.

reais ocorridos nas cidades de São Paulo e Rio de Janeiro. No primeiro caso, um homem ejaculou no pescoço de uma mulher no interior de um coletivo da capital paulista (METRÓPOLES, 2017). No segundo, uma mulher foi estuprada por trinta e três homens (GLOBO, 2016), sendo que as imagens foram divulgadas a partir de aplicativos de mensagens.

É cediço que a mídia exerce grande influência no Poder Legislativo brasileiro. Leis são criadas a partir de fatos, como se o Direito Penal representasse a solução para os problemas cotidianos. Monteiro (2015, p. 75) preleciona:

> [...] é necessário que se faça um estudo crítico dessa relação da Mídia com o Direito Penal, para demonstrar que isso resulta na deturpação da realidade criminal e, também, na criação de novos tipos penais mais severos, trazendo a ilusão de que a maior repressão poderá sanar a violência atual.

Em legislação esparsa, a Lei n.º 11.829, de 25 de novembro de 2008, inseriu ao Estatuto da Criança e do Adolescente (Lei n.º 8.069/90), entre outros, o artigo 241-A que disciplina:

> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.
> § 1º Nas mesmas penas incorre quem:
> I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;
> II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.
> § 2º As condutas tipificadas nos incisos I e II do § 1o deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo (BRASIL, 1990).

Como signatário da Convenção sobre os Direitos da Criança, adotada pela Assembleia Geral da Organização das Nações Unidas, de 20 de novembro de 1989, o Brasil fez sua parte e criminalizou a conduta de disponibilizar arquivos de pornografia infantojuvenil também pela *Internet.*

Com exceção das infrações em que a *Internet* é utilizada apenas como meio para a sua prática, a legislação sobre crimes explanada anteriormente constitui todo o arcabouço jurídico brasileiro acerca dos delitos virtuais. Entretanto, em pesquisa realizada no sítio da Câmara dos Deputados[5], existem atualmente cento e cinquenta e dois projetos de lei em tramitação para alteração do Código Penal, incluindo leis extravagantes que objetivam

[5]Disponível em: <https://www.camara.leg.br/busca-portal?contextoBusca=BuscaProposicoes&pagina=1&order=relevancia&abaEspecifica=true&filtros=%5B%7B%22descricaoProposicao%22%3A%22Projeto%20de%20Lei%22%7D,%7B%22temaPortal%22%3A%22Seguran%C3%A7a%22%7D%5D&q=INTERNET%20crime>. Acesso em 24 jun. 2022.

criminalizar novas condutas ou alterar crimes já existentes relacionados à *Internet.*

3 A LEGISLAÇÃO INTERNCIONAL SOBRE CRIMES CIBERNÉTICOS

Diversos países, de acordo com Rosendo (2007, p. 218), vêm legislando há considerável tempo a respeito do tema:

Quadro 1 – Legislação por países

País	Ano	Assunto
Alemanha	1986	Pirataria informática, alteração de dados, sabotagem de computadores etc.
Espanha	1995	Ataques que se produzem contra o direito de intimidade
Áustria	1987	Destruição de dados pessoais
Chile	1993	Lei n. 19223 (Lei de delitos informáticos, de 28 de maio de 1993)
França	1998	Lei n. 88-19 de 5 de janeiro de 1998
Estados Unidos	1986	Ata de fraude e abuso computacional
Itália	1993	Art. 615 Código Penal Italiano
Venezuela	2001	Lei Especial contra Delitos Informáticos (Diário Oficial n. 37.313 de 30 de outubro de 2001)
México	1999	Reforma do Código Penal Mexicano, Artigos 210 e 211
Bolívia	1997	Reforma do Código Penal Boliviano, Artigo 363
Costa Rica	2001	Lei 8148 que adicionou os artigos 196 bis, 217 bis e 229 bis ao Código Penal Costarriquenho
Peru	2001	Capítulo especial sobre delitos informáticos no Código Penal Peruano, Art. 207 e seguintes
Equador	2002	Lei de Comércio, Mensagens Eletrônicas e Mensagens Eletrônicas de Dados incorpora os artigos 184, 185, 186, 415 e 416 do Código Penal Equatoriano
Grã-Bretanha	1991	Lei de Abusos Informáticos
Portugal	1991	Lei Especial 109/1991
Japão	1987	Artigo 161 bis e seguintes

Fonte: ROSENDO. Eduardo E. Derecho Penal e informática. Buenos Aires: Fabián J Di Placido Editor, 2007.

Como anteriormente explanado, a criminalidade virtual não possui fronteiras. Com a finalidade de favorecer a repressão aos crimes praticados em ambiente virtual, em 23 de novembro de 2001 foi firmada, no âmbito do Conselho da Europa, a Convenção de Budapeste. Após as ratificações exigidas, quarenta e sete países membros do Conselho da Europa (quase a totalidade, já que a Europa é composta por cinquenta países), mais dezessete não membros (incluindo os sul-americanos Chile, Argentina e Colômbia), firmaram em Budapeste a Convenção sobre o Crime Cibernético. O Brasil aderiu à Convenção apenas em 2021, por

meio do decreto legislativo 255/2021.

A Convenção de Budapeste vislumbrou, em 2001, o crescimento da utilização dos meios eletrônicos como indispensáveis para a vida em sociedade, tanto que, ainda no preâmbulo, assim dispõe:

> Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation (EUROPA, 2001).

A Convenção de Budapeste sobre o Cibercrime visa, com prioridade, estabelecer uma política criminal comum entre os signatários. Intenta proteger a sociedade contra os delitos virtuais, adequando a legislação existente e melhorando a cooperação internacional, conforme consta em seu preâmbulo. Dispondo de tipificação de crimes em suas mais diversas modalidades, a Convenção também disciplina matéria de Direito Processual Penal a fim de possibilitar as condições necessárias para a elucidação do delito cibernético. Entretanto, para não se afastar do tema proposto ao presente estudo, este tópico serviu apenas para apresentar um breve panorama internacional acerca das leis penais sobre os crimes virtuais.

4 DA INVESTIGAÇÃO REALIZADA EM CRIMES PRATICADOS PELA *INTERNET* EM SANTA CATARINA

Em Santa Catarina, dados obtidos junto à Diretoria de Inteligência da Polícia Civil (SANTA CATARINA, 2019) demonstram o vertiginoso crescimento de apenas uma das modalidades de crimes praticadas na rede mundial de computadores, qual seja, a invasão de dispositivo informático. Foram analisados dados dos anos de 2017, 2018 e 2019 no que tange à formalização de Boletins de Ocorrência relacionados ao crime descrito no artigo 154-A do Código Penal. Comparando os registros, verificou-se que, no ano de 2017, foram registrados 358 Boletins de Ocorrência, enquanto que, em 2018, foram registrados 412 Boletins de Ocorrência referentes ao mencionado crime. Já em 2019, até o dia 09 de dezembro, foram formalizados 1292 Boletins de Ocorrência, o que revelou um acréscimo de mais de 313%.

Há que ressaltar, esses são os registros oficiais, excetuados os crimes em que não houve registro em Boletins de Ocorrência, bem como aqueles tipificados de forma diversa, quando a *Internet* foi utilizada apenas como meio para a prática delitiva, mas a infração já contava com tipificação penal.

Registrado o crime mediante Boletim de Ocorrência, a Polícia Civil inicia a investigação criminal. Assim como a maioria dos delitos, os crimes praticados por meio da *Internet* deixam vestígios. E estes, conforme explicam Velho, Costa e Damasceno (2013, p.

36) podem ser:

> [...] o conjunto de informações extraídas de um sistema computacional que permita esclarecer os fatos por trás de um crime ou fato em apuração, bem como os elementos físicos relacionados, que sirvam de suporte para o armazenamento, a produção ou o trânsito da informação.

A partir dos vestígios deixados pelo autor do crime e das obrigações legais que as provedoras de conexão à *Internet* possuem, desde o advento da Lei n.º 12.965/14, é possível identificar os protocolos de *Internet* (IPs) pelos quais trafegaram o criminoso. Esta informação, todavia, isolada de um aprofundamento investigativo não permite, por si só, a descoberta da autoria. O fato enseja uma maior complexidade quando o autor do crime cibernético é identificado por ato praticado fora do Brasil. Nesse caso, enfrenta-se um problema de soberania dos países para a obtenção dos dados necessários à completa identificação.

De acordo com Azambuja (2003, quando se diz que um Estado é soberano, isso significa que, em sua autoridade, o Estado é instado a realizar sua finalidade, qual seja, promover o bem público. Soberania significa que o poder do Estado é o mais elevado, superior a qualquer outro que ali existir. A soberania de um Estado afigura-se em dois aspectos: interno e externo. Soberania interna consubstancia-se no poder que o Estado possui mediante leis e ordens que edita para todos os que residem em seu território, bem como as sociedades e grupos formados por seus habitantes. Por sua vez, soberania externa significa que, entre os diferentes Estados, não há relações de subordinação e nem de dependência, mas sim de igualdade.

As diferentes Constituições e legislações penais espalhadas pelo mundo tendem a dificultar e/ou tornar sem efeito a persecução penal nos casos dos crimes cibernéticos. Na situação hipotética em que uma empresa tenha seu sistema invadido por um *software* malicioso que criptografou seus dados, exigindo determinada quantia em moeda virtual para o fornecimento da chave de descriptografia, em tese, tem-se a incidência dos artigos 154-A (invasão de dispositivo informático) e 158 (extorsão), ambos do Código Penal Brasileiro.

Ocorre que, realizadas as investigações preliminares, obtém-se ciência de que o autor utilizou protocolos de *Internet* sediados, por exemplo, na Rússia. Pesquisando o sítio do Ministério da Justiça e Segurança Pública, constata-se que o Brasil não possui acordo bilateral em matéria penal com a Rússia (JUSTIÇA, 2014). Há que ressaltar, a Lei 12.965/12 não é omissa nesse sentido. Entretanto, faz-se necessário o preenchimento de determinados requisitos. O artigo 11 assim disciplina:

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de Internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

> § 1º O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.
> § 2º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.
> § 3º Os provedores de conexão e de aplicações de Internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.
> § 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo (BRASIL, 2012).

Na hipótese antes mencionada, houve a prática de atos delitivos em território nacional (*caput*), pois um dos terminais está localizado no Brasil (§1º). Entretanto, a empresa não oferta serviço ao público brasileiro e não possui integrante do grupo econômico com estabelecimento no Brasil. Obviamente, neste exemplo, trata-se de um caso muito específico. Mais ainda quando as empresas de tecnologia possuem conglomerados internacionais em diversas partes do mundo.

No intuito de evitar situações extremadas, analisou-se um outro exemplo em que o mesmo crime foi praticado. Mas, desta vez, os protocolos de *Internet* estão sediados nos Estados Unidos e a empresa possui atuação no Brasil. Na hipótese em tela, os EUA possuem acordo bilateral em matéria penal com o Brasil, segundo o sítio do Ministério da Justiça e Segurança Pública. A questão agora reside em como obter tais dados e qual a real consequência, para o autor, dos atos criminosos praticados.

O Decreto n.º 3.810, de 2 de maio de 2001, regula o Acordo de Assistência em Matéria Penal entre o Governo da República Federativa do Brasil e o Governo dos Estados Unidos da América. Sobre o alcance da assistência, assim disciplina o Artigo I (BRASIL, 2001):

> 1. As Partes se obrigam a prestar assistência mútua, nos termos do presente Acordo, em matéria de investigação, inquérito, ação penal, prevenção de crimes e processos relacionados a delitos de natureza criminal.
> 2. A assistência incluirá:
> a) tomada de depoimentos ou declarações de pessoas;
> b) fornecimento de documentos, registros e bens;
> c) localização ou identificação de pessoas (físicas ou jurídicas) ou bens;
> d) entrega de documentos;
> e) transferência de pessoas sob custódia para prestar depoimento ou outros fins;
> f) execução de pedidos de busca e apreensão;
> g) assistência em procedimentos relacionados a imobilização e confisco de bens, restituição, cobrança de multas; e
> h) qualquer outra forma de assistência não proibida pelas leis do Estado Requerido.
> 3. A assistência será prestada ainda que o fato sujeito a investigação, inquérito ou ação penal não seja punível na legislação de ambos os Estados.
> 4. As Partes reconhecem a especial importância de combater graves

> atividades criminais, incluindo lavagem de dinheiro e tráfico ilícito de armas de fogo, munições e explosivos. Sem limitar o alcance da assistência prevista neste Artigo, as Partes devem prestar assistência mútua sobre essas atividades, nos termos deste Acordo.
> 5. O presente Acordo destina-se tão-somente à assistência judiciária mútua entre as Partes. Seus dispositivos não darão direito a qualquer indivíduo de obter, suprimir ou excluir qualquer prova ou impedir que uma solicitação seja atendida.

No presente exemplo, praticado o crime com protocolos de *Internet* sediados nos Estados Unidos, o delegado de polícia representará ao Poder Judiciário para que as informações sejam prestadas e, com a decisão judicial, dará início ao trâmite necessário para o envio da documentação. Em sede de cumprimento, disciplina o Artigo V, 1:

> A Autoridade Central do Estado Requerido atenderá imediatamente à solicitação ou a transmitirá, quando oportuno, à autoridade que tenha jurisdição para fazê-lo. As autoridades competentes do Estado Requerido envidarão todos os esforços no sentido de atender à solicitação. A justiça do Estado Requerido deverá emitir intimações, mandados de busca e apreensão ou outras ordens necessárias ao cumprimento da solicitação.

Ocorre que, na prática, essas “eficiência e agilidade” não são observadas. Conforme Grossmann (2018), o Ministério Público Federal, por meio da Procuradoria Geral da República, já informou que, dos 108 pedidos de colaboração jurídica com os Estados Unidos para obtenção de dados telemáticos, apenas 18 foram atendidos. Portanto é possível observar que, apesar da regulação legislativa mediante a Lei n.º 12.965/14, o instrumento de operacionalização é deficitário. Na prática, não dispõe da pretendida eficiência que está disposta na legislação.

De outro lado, alguns autores, como Bergmann (2016), sustentam que não haveria necessidade de obter informações a partir do acordo em matéria penal, pois o seu local de armazenamento não está relacionado à possibilidade de acesso. Ademais, caso a filial não tivesse autorização para fazê-lo, pediria à matriz que os repassasse.

Concernente ao argumento de que os dados estão na sede da empresa situada nos Estados Unidos, como no exemplo citado, Bergmann (2016, p. 43) esclarece:

> As maiores e mais conhecidas empresas que fornecem serviços na Internet possuem *data centers* (centros de processamento de dados onde estes são armazenados em computadores ou dispositivos de grande capacidade) espalhados por diversas regiões do mundo. É uma medida de segurança (em caso de catástrofes naturais, por exemplo) e de economia (mão de obra e/ou energia mais barata, incentivos fiscais, etc) adotada pelas empresas.

Esse posicionamento encontra respaldo na jurisprudência, tanto que o Superior Tribunal de Justiça já decidiu (BRASIL, 2019):

> [...] por estar instituída e em atuação no País, a pessoa jurídica multinacional submete-se, necessariamente, às leis brasileiras, motivo pelo qual se afigura desnecessária a cooperação internacional para a obtenção dos dados

> requisitados pelo juízo.

Nesse mesmo sentido, extrai-se do egrégio Tribunal de Justiça do Estado de Santa Catarina (SANTA CATARINA, 2010a):

> [...] a apelante tem à sua disposição os dados telemáticos, ao passo que o cumprimento da obrigação é plenamente viável. Note-se que a satisfação da condenação poderá ocorrer por simples comunicação interna entre a apelante (subsidiária) e a sede, pois, conforme explicitado, o Google não faz qualquer distinção e divisão de atribuições (material e territorial) na prestação dos serviços.

A Corte Catarinense também já se manifestou acerca do caráter multinacional dos provedores de aplicação (SANTA CATARINA, 2010b):

> A apelante desenvolve atividade empresarial de provedor de aplicação de Internet no Brasil, a qual pode ter pleno acesso aos bancos de dados - que estão arquivados pelo Google, Inc. em virtude do ajuizamento da medida cautelar -, considerando se tratar de empresa multinacional e que detém grande poder econômico.

Independentemente do posicionamento que se adote, o fato é que a matéria é controversa e necessita de maior e melhor regulamentação por parte do legislador. Não há como admitir que crimes venham a ser praticados em solo brasileiro e as autoridades responsáveis encontrem dificuldades na obtenção dos dados necessários à sua elucidação.

Oportuno observar que essas decisões são em grau de recurso, ou seja, os provedores de aplicação e/ou de conexão à *Internet* não forneceram as informações necessárias a partir da decisão exarada pelo magistrado de primeiro grau. Ou seja, insurgiram-se contra a decisão e recorreram ao Tribunal para negar o fornecimento. Tal situação em sede de investigação mostra-se extremamente prejudicial, pois o tempo decorrido desde a decisão até a real obtenção da informação pode fazer com que não se produzam os elementos informativos necessários para a prova de materialidade e os indícios suficientes de autoria.

O fato é que a regulamentação precisa ser eficaz e englobar as mais corriqueiras práticas criminosas perpetradas em ambiente virtual, sob pena de subsistirem crimes sem a devida persecução penal.

5 CONSIDERAÇÕES FINAIS

A sociedade tem alterado significativamente sua forma de viver, por conta dos meios ofertados pela tecnologia. As inovações são quase que diárias e afetam a vida de todos, seja para beneficiá-los, seja para prejudicá-los. O Estado, como regulador da vida em sociedade, precisa também participar desse processo e observar as condutas criminosas que podem ser trazidas junto com a tecnologia. Não há como permanecer de modo inerte até que o crime se configure e, só então, ir em busca de uma legislação penal eficiente.

A ausência de fronteiras que a *Internet* propicia enseja um esforço mundial na regulamentação de legislações específicas sobre o tema, a fim de atribuir responsabilidade às empresas, bem como identificar e penalizar os autores de atos criminosos praticados em ambiente virtual.

Autores citados no presente trabalho, como Nogueira (2016) e Monteiro (2015) concordam que o recrudescimento da legislação interna de cada país com relação aos fatos ocorridos na rede mundial de computadores deva estar intimamente ligado às políticas das empresas que exploram tal atividade econômica. O esforço necessita ser conjunto e voltado para o bem-estar do usuário, o qual não pode ficar à mercê de um *click* equivocado e ter a sua vida devassada ou os seus bens lesados.

De outro lado, a educação digital também se afigura como de fundamental importância para que a sociedade tenha conhecimento das formas de agir no ambiente virtual. A partir do momento em que as pessoas efetivamente conhecem a ferramenta que utilizam, sabem qual a sua funcionalidade e quais os cuidados que precisam ter em seu manuseio.

Por sua vez, as inovações continuarão a acontecer. Desse modo, cabe também a cada um buscar o conhecimento necessário para não se tornar mais uma vítima de crimes virtuais (em contínuas inovações), em um mundo, diga-se, cada vez mais digital.

REFERÊNCIAS

AZAMBUJA, Darcy. **Teoria geral do Estado**. 4 ed. rev., ampl. e atual. – São Paulo: Globo, 2018.

BERGMANN, Pablo Barcellos. **Aspectos penais do Marco Civil da Internet**. In: BEZERRA, Cleiton da Silva/AGNOLETTO, Giovani Celso (org.). *Combate ao Crime Cibernético - Doutrina e Prática (A Visão do Delegado de polícia)*. 1. ed.- Rio de Janeiro: Mallet Editora, 2016.

BRASIL. CÂMARA DOS DEPUTADOS. (Comp.). **Projetos de Lei. 2019**. Disponível em: < https://www.camara.leg.br/busca-portal?contextoBusca=BuscaProposicoes&pagina=1&order=relevancia&abaEspecifica=true&q=ciber%20crime&tipos=PEC,PLP,PL,MPV,PLV,PDL,PRC,REQ,RIC,RCP,MSC,INC >. Acesso em: 05 abr. 2022.

BRASIL. **Decreto Nº 3.810, de 2 de maio de 2001**. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/2001/D3810.htm>. Acesso em: 25 jun. 2022.

BRASIL. **Decreto-Lei Nº 2.848, de 7 de dezembro de 1940**. Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em: 25 jun. 2022.

BRASIL. **Lei nº 7.716, de 5 de janeiro de 1989**. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l7716.htm>. Acesso em: 25 jun. 2022.

BRASIL. **Lei nº 9.983, de 14 de julho de 2000**. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L9983.htm>. Acesso em: 25 jun. 2022.

BRASIL. **Lei nº 12.735, de 30 de novembro de 2012**. Disponível em:

<http://www.planalto.gov.br/ccivil_03/ _Ato2011-2014/2012/Lei/L12735.htm>. Acesso em: 25 jun. 2022.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 25 jun. 2022.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 25 jun. 2022.

BRASIL. **Lei nº 13.718, de 24 de setembro de 2018**. Disponível em: <http://www.planalto.gov.br/ccivil_03 _ato2015-2018/2018/lei/L13718.htm>. Acesso em: 25 jun. 2022.

BRASIL. Superior Tribunal de Justiça. **Recurso em Mandado de Segurança: RMS 55.109/PR**, Relator: Ministro Reynaldo Soares da Fonseca. DJ: 17/11/2017.

CARNEIRO, Adeneele Garcia. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. **Âmbito Jurídico**, Rio Grande, XV, n.99, abr. 2012. Disponível em:< https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-uma-reflexao-sobre-o-problema-na-tipificacao/>. Acesso em: 05 abr. 2022.

EUROPA. Convenção (2001). **Convenção de 23 de novembro de 2001**. Convenção de Budapeste 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: 26 nov. 2019.

FMP. **Lei Carolina Dieckmann**: você sabe o que essa lei representa? Disponível em: <https://fmp.edu.br/lei-carolina-dieckmann-voce-sabe-o-que-essa-lei-representa/> . Acesso em 05 abr. 2022.

GLOBO. **Vítima de estupro coletivo no Rio conta que acordou dopada e nua**, 2016. Disponível em: <http://g1.globo.com/rio-de-janeiro/noticia/2016/05/vitima-de-estupro-coletivo-no-rio-conta-que-acordou-dopada-e-nua.html>. Acesso em: 25 jun. 2022.

GOGONI, Ronaldo. **E a palavra do ano do Dicionário Oxford é... um emoji**. 2015. Disponível em: <https://meiobit.com/331218/dicionario-oxford-palavra-do-ano-2015-emoji/>. Acesso em: 25 jun. 2022.

GROSSMANN, Luís Osvaldo. Para PGR, **MLAT não pode ser único recurso para acesso a dados no exterior**. 2018. Disponível em: <https://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=47775&sid=4>. Acesso em: 09 dez. 2019.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). **Pesquisa Nacional por Amostra de Domicílios Contínua (Pnad C) 2018**. Rio de Janeiro. Disponível em <https://biblioteca.ibge.gov.br/visualizacao/livros/liv101548_notas_tecnicas.pdf>. Acesso em 25 jun. 2022.

JUSTIÇA. **Cooperação Jurídica Internacional em matéria penal.** Disponível em: <https://www.justica.gov.br/sua-protecao/cooperacao-internacional/cooperacao-juridica-internacional-em-materia-penal/acordos-internacionais/acordos-bilaterais-1> Acesso em: 25 jun. 2022.

METRÓPOLES. **Homem é preso após ejacular no pescoço de uma mulher dentro do ônibus**. 2017. Disponível em: <https://www.metropoles.com/brasil/homem-e-preso-apos-ejacular-no-pescoco-de-uma-mulher-dentro-do-onibus/amp>. Acesso em: 27 nov. 2019.

MONTEIRO, Midiã. **A influência da mídia na expansão da legislação penal no Brasil**. 2015. Disponível em: <https://jus.com.br/artigos/38271/a-influencia-da-midia-na-expansao-da-legislacao-penal-no-brasil>. Acesso em: 25 jun. 2022.

NOGUEIRA, Luiz Augusto Pessoa. **Dos crimes cibernéticos (Lei 12.737/12).** In: BEZERRA, Cleiton da Silva/AGNOLETTO, Giovani Celso (org.). *Combate ao Crime Cibernético - Doutrina e Prática (A Visão do Delegado de polícia)*. 1. ed.- Rio de Janeiro: Mallet Editora, 2016.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Cibercrime movimenta US$1,5 trilhão por ano, diz ONU. 2018**. Disponível em: <https://nacoesunidas.org/cibercrime-movimenta-us15-trilhao-por-ano-diz-onu/>. Acesso em: 14 jan. 2019.

PADILHA, Felipe. **O que é *emoji*.** Disponível em: <https://www.significados.com.br/emoji/>. Acesso em: 25 jun. 2022.

PINHEIRO, Patrícia Peck. **Direito Digital**. São Paulo: Saraiva. 2010.

ROSENDO. Eduardo E. **Derecho Penal e informática**. Buenos Aires: Fabián J Di Placido Editor. 2007.

SANTA CATARINA. Polícia Civil. Secretaria do Estado da Segurança Pública**. Boletins de Ocorrência**. 2019. Disponível em: <www.pc.sc.gov.br>. Acesso em: 09 dez. 2019.

SANTA CATARINA. Tribunal de Justiça do Estado de Santa Catarina. **Embargos de Declaração nº 0025584-20.2010.8.24.0020**. Relator: Desembargador Rubens Schulz. Florianópolis, SC, 27 de junho de 2019.

SANTA CATARINA. Tribunal de Justiça do Estado de Santa Catarina. **Apelação Cível nº 0025584-20.2010.8.24.0020**. Relator: Desembargador Rubens Schulz. Florianópolis, SC, 02 de maio de 2019.

TOBARES, Gabriel H. Catala. **Delitos Informaticos**. Cordoba: Advovatus. 2010.

VELHO, J. A; COSTA. K. A.; DAMASCENO, C. T.M. **Locais de Crimes** - Dos Vestígios à Dinâmica Criminosa. 1. ed. Campinas: Millenium, 2013.