O ENFRENTAMENTO DO *CIBERCRIME* ENTRE A COOPERAÇÃO INTERNACIONAL E A EXPANSÃO DO DIREITO PENAL[†]

Cláudio Macedo de Souza[1]

Hugo Leonardo Barboza [2]

Resumo: Este artigo objetiva investigar a expansão do Direito Penal no contexto da política criminal imersa na ideia de risco representada pela criminalidade cibernética. Nesta perspectiva, questionou-se: "Qual efeito a tipificação penal contra o *cibercrime* produz na ordem jurídica interna dos Estados signatários da Convenção de Budapeste?" Assumiu-se como hipótese de pesquisa que a tipificação de novos tipos legais mediante processo de harmonização da legislação penal gera expansão do Direito Penal em razão da política criminal fundamentada na transnacionalidade do crime. Inicialmente, apresentou-se a categoria dos crimes cibernéticos e sua pertinência para a cooperação internacional em matéria penal. Em seguida, investigou-se a possibilidade de expansão do Direito Penal como resultado de eventual adesão à Convenção de Budapeste. Para tanto, adotou-se o método hipotético-dedutivo, sustentado pela revisão bibliográfica. Como resultado, identificou-se que o processo de harmonização legislativa para adesão à Convenção de Budapeste provocaria expansão do Direito Penal, com novos tipos penais para os

[†] Este artigo faz parte do projeto "Escola de Altos Estudos em Inovações Jurídicas para o direito das gerações futuras na América Latina" e é resultado de pesquisa financiada pelo CNPq.

[1] Professor de Direito Penal na UFSC - Universidade Federal de Santa Catarina nos cursos de Graduação e de Pós-graduação em Direito. Possui Especialização e Doutorado em Ciências Penais pela UFMG - Universidade Federal de Minas Gerais.

[2] Mestrando em Direito pela Universidade Federal de Santa Catarina (UFSC). Graduado em Direito pela Universidade Estadual de Maringá (UEM).

crimes cibernéticos.

Palavras-Chave: *Cibercrime*; Cooperação Internacional; Harmonização; Expansão.

THE ENGAGEMENT AGAINST CYBERCRIME BETWEEN INTERNATIONAL COOPERATION AND THE EXPANSION OF CRIMINAL LAW

Abstract: This article aims to investigate the expansion of Criminal Law in the context of criminal policy affected by the idea of risk, represented by cybercrime. In this regard, the question of this research is: what effect does the criminal typification against cybercrime have on the domestic legal order of Budapest Convention's signatory states? It was assumed as a hypothesis that the typification of new legal types through the process of harmonization of criminal legislation engenders an expansion of Criminal Law due to the criminal policy based on the transnationality of the crime. Initially, the category of cybercrimes and their relevance to international cooperation in criminal matters was presented. Then, it was investigated the possibility of expansion of Criminal Law due to an eventual adhesion to the Budapest Convention. Therefore, the hypothetical-deductive method was adopted, supported by the literature review. As a result, it was identified that the process of legislative harmonization for accession to the Budapest Convention would produce an expansion of the Criminal Law, creating new criminal types for cybercrimes.

Keywords: Cybercrime; International Cooperation; Harmonization; Expansion.

INTRODUÇÃO

Este artigo objetiva compreender a possibilidade de expansão do Direito Penal como resultado da política criminal associada à cooperação internacional em matéria penal prevista na Convenção de Budapeste. Tratado internacional de direito penal e direito processual penal, o documento sobre o *Cibercrime*, foi firmado no âmbito do Conselho da Europa para definir de forma harmônica os crimes praticados por meio da *Internet* e as formas de persecução a nível transnacional. Para garantir um arcabouço jurídico comum entre os países nesta área, o documento prevê os países signatários cooperarão entre si com base em legislações uniformes para efeitos de investigações ou de procedimentos relativos a infracções penais relacionadas com sistemas e dados informáticos[3].

A partir dessa constatação, observa-se que a harmonização da legislação penal foi eleita como princípio geral relativo à cooperação jurídica internacional para o enfrentamento da criminalidade praticada pela *internet*. Os crimes cibernéticos, entre os quais estão desde a pirataria de conteúdos audiovisuais, violação de dados, fraudes e até pornografia infantil, são cada vez mais internacionais, com os criminosos e vítimas estabelecidos em países diversos de modo a exigir uma cooperação cada dia mais eficiente.

A informação, o armazenamento de dados e seu processamento adquirem na atualidade um valor estratégico não apenas

[3] Essa diretriz está prevista no artigo 23 e, também, no Preâmbulo da Convenção de Budapeste, conforme texto transcrito a seguir: "The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international cooperation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence". CONSELHO DA EUROPA. *Convention on Cybercrime*. 2001. Disponível em: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>. Acesso em: 20/06/2021.

no âmbito da intimidade das pessoas, mas também circunscreve à sua funcionalidade, que transcende a esfera meramente individual e se projeta sobre o funcionamento de uma sociedade de mercado. que imprime a necessidade de adotar medidas legais para sua correta tutela. Portanto, não se pode ignorar a existência de uma política criminal comum voltada à tutela penal da informação, sobretudo, no atual contexto da pandemia de Covid-19 em que a atividade humana mundial está inserida num progressivo processo de digitalização. E, a busca por uma política criminal comum possibilita a criação de novos tipos legais, ainda não previstos na ordem jurídico-penal.

O risco de que as redes informáticas e a informação electrónica possam ser utilizadas para a prática de infrações criminais e de que as provas dessas infrações possam ser armazenadas e transmitidas através dessas redes é preocupação de destaque prevista no preâmbulo da Convenção[4]. O risco representado pela criminalidade cibernética apresenta desafios multitemáticos que frequentemente extrapolam as fronteiras físicas dos Estados. Nesta direção, é preciso atentar, especialmente, para o caráter transfronteiriço do crime que se utiliza de serviços de fora da jurisdição dos países, dentre os quais o Brasil.

A origem do problema gravita em torno da necessidade do Estado de garantir o acervo normativo harmonizado no âmbito doméstico para o enfrentamento dessa criminalidade cujo risco é destacado em função da sua transnacionalidade. Diante disso, exige-se, em escala global, a tipificação penal de condutas em conformidade com a Convenção a fim de que a cooperação jurídica internacional em matéria penal se desenvolva.

Neste sentido, indagou-se no presente artigo: "Qual

[4] Preâmbulo da Convenção de Budapeste: "Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks". CONSELHO DA EUROPA. *Convention on Cybercrime*. 2001. Disponível em: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>. Acesso em: 20/06/2021.

efeito a tipificação penal contra o *cibercrime* produz na ordem jurídica interna dos Estados signatários da Convenção de Budapeste?" Ofertou-se, assim, uma solução ao problema formulado com a seguinte resposta preliminar: "A tipificação de novos tipos legais mediante o processo de harmonização da legislação penal produz expansão da ordem jurídica em decorrência da política criminal fundamentada no risco representado pelo *cibercrime*".

Na esteira de uma política criminal reativa aos espaços de riscos jurídicos penalmente relevantes, existe a preocupação com a formação de um Estado de polícia próprio ao ciberespaço, em razão da possibilidade concreta de aumento do poder punitivo, incompatível com princípios basilares do Estado de Direito. Afirma-se, pois, que as principais causas da expansão do poder punitivo estatal são o efetivo surgimento de novos riscos trazidos pela sociedade pós-industrial, e o sentimento geral de insegurança social.

Parece não haver dúvida de que a informação deve ser objeto de tutela de um Direito Penal orientado para evitar riscos. Todavia, a ideia de risco representada pelo *cibercrime* pode produzir, especialmente, a criminalização de novos bens jurídicos, o incremento da sanção penal, o aumento de tipos de perigo abstrato e de normas penais em branco, a flexibilização das regras de imputação e a relativização das garantias processuais.

O artigo ofertado à leitura foi construído em dois momentos. Inicialmente, buscou-se investigar o potencial ofensivo dos crimes virtuais, bem como o modelo de cooperação internacional em torno da Convenção de Budapeste. Para tanto, foi avaliado o conteúdo das principais normas domésticas e internacionais referentes ao tema, em especial, aquelas previstas na Convenção de Budapeste.

No segundo momento, examinou-se o fenômeno da expansão do Direito Penal enquanto efeito global causado pela política criminal inserida no âmbito da Convenção de Budapeste.

Ademais, a fim de ilustrar a relação entre a ideia do risco e a transnacionalidade da criminalidade cibernética, o artigo considerou diversos documentos internacionais nos quais a rede informática é caracterizada por prestar um serviço de comunicação que não conhece as tradicionais fronteiras estatais.

Investigou-se, ainda, a existência de processo emergente de formação de um Estado de polícia no âmbito do ciberespaço, e consequentemente sua destacada incompatibilidade com o Estado Democrático de Direito. Nessa perspectiva, o Direito Penal, frente aos novos riscos, já não cumpriria uma função de proteção fragmentária e subsidiária de bens jurídicos, senão que se transformaria em um instrumento de governo ou de grupos defensores de determinados interesses.

OS CRIMES CIBERNÉTICOS E A COOPERAÇÃO INTERNACIONAL EM MATÉRIA PENAL

O surgimento das novas tecnologias de informação e de comunicação provocou transformações nas relações sociais e, consequentemente, reflexão em torno de um Direito Penal cada dia mais preventivo para o enfrentamento dos crimes virtuais[5]. Nessa perspectiva, o Direito Penal frente aos riscos do *cibercrime* já não cumpriria uma função de proteção fragmentária e subsidiária, pois a técnica de tipificação desses crimes, mais compatível com os anseios de antecipação máxima da proteção penal, seria a do perigo abstrato. Essa tendência intervencionista, punitivista e de hipertrofia na era da globalização destaca, com propriedade, os "riscos do Direito Penal do risco".

As relações sociais desenvolvidas em torno das crescentes interações transnacionais, envolvendo atores públicos ou

[5] "Não são poucas as leis que contemplam uma criminalização exageradamente antecipada em relação à lesão do bem jurídico, o que ocorre com frequência para a prevenção de riscos aos bens coletivos ou supraindividuais." GOMES, Luiz Flávio et al. Direito Penal - introdução e princípios fundamentais. V. 1. São Paulo: Revista dos Tribunais, 2007, p. 345.

privados que demarcam a globalização, são caracterizadas pela expansão dos fluxos financeiros, pela internacionalização e pela nova divisão do trabalho, pela ampliação das redes de comunicação e pela redução das fronteiras físicas[6]. No marco de desenvolvimento das sociedades pós-industriais que ostentam o difuso estandarte da globalização, a criminalidade informática recria um novo horizonte para o Direito Penal, tendo em vista o aumento dos fluxos internacionais de dados e informações em diversas partes do mundo.

Este cenário expõe aos governos a existência de forças com alto impacto na vida da população e que não estão necessariamente dentro de seu campo de controle[7]. A globalização, entendida sob uma perspectiva negativa, portanto, insere aspectos de risco ao espectro social e político, os quais podem ser caracterizados como as inseguranças e vulnerabilidades oriundas da contemporaneidade[8].

Na sociedade de risco, a preocupação com as inseguranças gera desconfortos com a própria percepção do futuro, isto é, com fenômenos que ainda não se concretizaram no plano fático[9]. O *cibercrime*, em relação a este ponto, pode ser considerado como um dos riscos que produz este sentimento de insegurança na sociedade.

Essa conjuntura atribui ao direito e ao sistema judicial a responsabilidade de garantir a ordem, a previsibilidade e a confiança nas relações sociais. Com a finalidade de promover a garantia adequada, é necessário haver "um conjunto de instituições independentes e universais que criam expectativas normativamente fundadas e resolvem litígio em função de quadros legais

---

[6] SANTOS, Boaventura de Sousa. *A globalização e as ciências sociais*. São Paulo: Cortez. 2002, p. 25-27.

[7] HOBSBAWN, Eric. *Globalização, democracia e terrorismo*. Tradução: José Viegas. São Paulo: Companhia das letras, 2007, p. 109.

[8] BECK, Ulrich. *La sociedad del riesgo: Hacia una nueva modernidad*. Barcelona: Paidós Ibérica, 2006, p. 21.

[9] BECK, Ulrich. *La sociedad del riesgo: Hacia una nueva modernidad*. Barcelona: Paidós Ibérica, 2006, p. 40.

presumivelmente conhecidos de todos"[10].

O relatório explicativo para a Convenção sobre *Cibercrime* se atenta aos riscos de uso das novas tecnologias, em especial das tecnologias de informação e de comunicação, para novos tipos de crimes e para a prática dos crimes tradicionais, mas pela via digital[11]. O relatório complementa:

> As novas tecnologias desafiam os conceitos legais existentes. Informações e comunicações fluem mais facilmente ao redor do mundo. Fronteiras já não são mais limitações para esse fluxo. Criminosos estão cada vez mais localizados em regiões diferentes daqueles onde suas condutas produzem efeitos. No entanto, as leis domésticas estão normalmente confinadas em um território específico. Assim, soluções para os problemas apresentados precisam ser direcionadas pelo Direito Internacional, de modo que necessite a adoção de instrumentos internacionais adequados [...] (tradução nossa)[12].

O Escritório das Nações Unidas sobre Drogas e Crime (UNODC) concluiu que o aumento da conectividade global contribuiu para o desenvolvimento da criminalidade cibernética contemporânea, na medida em que tais atividades fazem uso das tecnologias de informação de alcance global para a prática de crimes em escala transnacional[13].

---

[10] SANTOS, Boaventura de Sousa. *A globalização e as ciências sociais*. São Paulo: Cortez. 2002, p. 43.

[11] CONSELHO DA EUROPA. *Explanatory Report to the Convention on Cybercrime*. 2001, p. 1-2. Disponível em: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b>. Acesso em: 20/06/2021.

[12] Versão original: The new technologies challenge existing legal concepts. Information and communications flow more easily around the world. Borders are no longer boundaries to this flow. Criminals are increasingly located in places other than where their acts produce their effects. However,domestic laws are generally confined to a specific territory. Thus solutions to the problems posed must be addressed by international law, necessitating the adoption of adequate international legal instruments. CONSELHO DA EUROPA. *Explanatory Report to the Convention on Cybercrime*. 2001, p. 2. Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b. Acesso em: 20/06/2021.

[13] ESCRITÓRIO DAS NAÇÕES UNIDAS SOBRE DROGAS E CRIME. *Comprehensive Study on Cybercrime*. United Nations: Viena, 2013, p. 4. Disponível em:

Crimes virtuais, crimes cibernéticos, e *cibercrimes* são terminologias intercambiáveis. Todavia, são apenas alguns dos rótulos utilizados pela linguagem dogmática para sintetizar o crescente fenômeno da criminalidade informática e informatizada. O Direito Penal informático é manifestação recente e seu desenvolvimento histórico revela uma permanente adaptação às novas tecnologias. Por isso, torna-se essencial definir conceitos e condutas que integram os crimes cibernéticos. Cita-se, por exemplo, invasões de banco de dados, clonagem de perfis, estelionato e o desvio de fundos previdenciários[14].

O conteúdo e alcance das terminologias citadas acima está relacionada à priorização do envolvimento da *internet* nas condutas desta criminalidade. O cibercrime, em sentido estrito, faz referência aos "crimes cometidos contra um computador ou fazendo uso de um computador"[15].

Os crimes cibernéticos, nesse sentido, fazem da *internet* e das tecnologias de rede uma relevante ferramenta. É a partir desta relação que as terminologias "crime cibernético" ou "cibercrime" ganham prevalência, uma vez que dão maior ênfase ao uso da *internet* e das redes[16]. Mas, a conceituação do crime deveria ser ampla para abarcar tanto as modalidades que utilizam um sistema informático como meio para a prática dos mais variados ilícitos quanto nos casos em que o referido sistema se

https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf. Acesso em 14/06/2021.

[14] CASTRO, José Roberto Wanderley. *A tipicidade dos crimes cibernéticos no direito penal brasileiro: um estudo sobre o impacto da Lei 12.737/2012 e a (des)construção de uma dogmática penal dos crimes cibernéticos*. 2018. 231f. Tese (doutorado) – Universidade Federal de Pernambuco. Recife, 2018, p. 112.

[15] WANG, Qianyun. *A Comparative Study of Cybercrime in Criminal Law: China, US, England, Singapore and the Council of Europe*. Tese (doutorado) – Erasmus University Rotterdam. Rotterdam, 2016, p. 5-7. Versão original: 'Virtual crime', in its narrower sense, equates to 'cybercrime', and refers to 'crimes committed against a computer or by means of a computer'.

[16] WANG, Qianyun. *A Comparative Study of Cybercrime in Criminal Law: China, US, England, Singapore and the Council of Europe*. Tese (doutorado) – Erasmus University Rotterdam. Rotterdam, 2016, p. 7.

transforma em objeto do comportamento delitivo.

Segundo o relatório "*Internet Organised Crime Threat Assessment*", desenvolvido pela EUROPOL, os agentes do crime conseguem atuar em alta velocidade, uma vez consideradas as tecnologias decorrentes da *internet*. Assim, conseguem atuar e interferir na infraestrutura de determinado sistema, de alterar códigos, de adaptar funcionalidades ou de obter informações das vítimas, por exemplo. O crime é um desafio central, pois seus autores conseguem atingir um número considerável de vítimas potenciais sem despender grandes investimentos, além de obterem vantagens econômicas evidentes[17].

A manipulação de dados, de modo a interferir no fluxo de entrada e saída de dados dos sistemas computacionais é apenas parte das espécies de condutas ilícitas. A doutrina faz, também, referência às práticas de espionagem, mediante subtração de dados e informações. Há, ainda, a sabotagem, na qual está o interesse de destruir parcial ou integralmente determinado *software* ou *hardware*. Entretanto, condutas como as destacadas não encontram amparo legislativo adequado no Direito Penal clássico[18]. Há, portanto, a necessidade de se repensar o sistema jurídico-penal a ser aplicado em relação aos crimes cibernéticos.

O UNODC exemplifica o alcance das definições de *cibercrime*:

> [...] incluindo fraudes relacionadas ao uso do computador e roubos de identidade; produção computadorizada, distribuição e armazenamento de pornografia infantil; tentativas de *phishing*; e acesso ilegal a sistemas de computadores, incluindo *hacking* (tradução nossa)[19].

---

[17] EUROPOL. *Internet Organized Crime Threat Assessment (IOCTA)*. European Agency for Law Enforcement Cooperation. 2020, p. 12-17. Disponível em: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020. Acesso em 14/06/2021.

[18] CASTRO, José Roberto Wanderley. *A tipicidade dos crimes cibernéticos no direito penal brasileiro: um estudo sobre o impacto da Lei 12.737/2012 e a (des)construção de uma dogmática penal dos crimes cibernéticos*. 2018. 231f. Tese (doutorado) – Universidade Federal de Pernambuco. Recife, 2018, p. 106.

[19] ESCRITÓRIO DAS NAÇÕES UNIDAS SOBRE DROGAS E CRIME.

Definir uma definição adequada não é simples, porque existem várias abordagens distintas para caracterizar o fenômeno, o qual pode ser usado com a finalidade de englobar igualmente os crimes de computador e aqueles que fazem uso das redes e conexões[20].

É necessário apresentar critérios práticos para melhor compreender os tipos penais da criminalidade cibernética. A Convenção de Budapeste sobre *Cibercrime* apresenta 4 (quatro) situações típicas para sua compreensão: condutas ofensivas à confidencialidade, integridade e disponibilidade de dados ou sistemas de computador; crimes relacionados com computadores; crimes relacionados com o conteúdo; e crimes relacionados com direitos autorais[21].

O aspecto central para a compreensão dos crimes cibernéticos é identificar os bens jurídicos, com destaque para duas possibilidades de ofensa. Em primeiro lugar, cite-se a hipótese de crime praticado pela via digital em que o bem jurídico ofendido será diferente do sistema informático em si, como o patrimônio. Outra modalidade de ofensa diz respeito às condutas praticadas contra o sistema de informação, ou crime cibernético

---

Comprehensive Study on Cybercrime. United Nations: Viena, 2013, p. 8. Disponível em: https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf. Acesso em 14/06/2021. Versão original: [...] including computer-related fraud and identity theft; computer-related production, distribution, or possession of child pornography; phishing attempts; and illegal access to computer systems, including hacking (UNODC, 2013, p. 8). O estudo elaborado pelo UNODC classifica os crimes cibernéticos em condutas contra a confidencialidade, integridade ou disponibilidade de dados ou sistemas de computador; condutas computadorizadas com a finalidade de obter ganhos financeiros ou de gerar prejuízos; e condutas relacionadas ao conteúdo veiculado ou armazenado em computadores (2013, p. 16).

[20] INTERNATIONAL TELECOMMUNICATION UNION. *Understanding Cybercrime: Phenoma, challenges and legal response*. ITU: 2012, p. 12. Disponível em: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf. Acesso em 14/06/2021.

[21] INTERNATIONAL TELECOMMUNICATION UNION. *Understanding Cybercrime: Phenoma, challenges and legal response*. ITU: 2012, p. 12. Disponível em: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf. Acesso em 14/06/2021.

próprio, a partir dos quais existe tendência de se considerar o sistema informático como bem jurídico[22].

Sobre os bens jurídicos ofendidos, Santos destaca:

> "Os bens jurídicos lesionados por meio da internet podem ser tanto o sistema informático em si mesmo, os dados pessoais arquivados ou disponibilizados por meio do sistema informático, como ainda outros bens jurídicos lesionados em razão do conteúdo veiculado por meio do sistema informático (publicidade enganosa e abusiva, pornografia infantil), e que devem ser tipificados penalmente"[23].

Qianyun Wang classifica os crimes em 3 (três) grupos. A primeira classificação se refere aos crimes nos quais o computador ou a rede de computadores é o alvo da conduta. A segunda está associada aos crimes tradicionais nos quais os

---

[22] A distinção entre os crimes cibernéticos próprios e impróprios é avaliada por Castro. Nesse ponto, o autor retoma Damásio de Jesus e José Antônio Milagre para aprofundar a classificação, cuja terminologia adotada, de maneira geral, é "crimes informáticos". Os próprios são aqueles em que a tecnologia da informação é o objeto material sobre o qual recai a conduta do sujeito ativo. Os impróprios, ademais, são aqueles em que "a tecnologia da informação é o meio utilizado para a agressão aos bens jurídicos já protegidos pelo Código Penal Brasileiro". Os crimes informáticos mistos englobam condutas complexas, que violam o bem jurídico informático e um outro bem jurídico específico – trata-se, nesse sentido, da ocorrência de dois tipos penais distintos. Já mediatos ou indiretos, por fim, compreendem os crimes informáticos que decorrem da prática de ilícito não informático. CASTRO, José Roberto Wanderley. *A tipicidade dos crimes cibernéticos no direito penal brasileiro: um estudo sobre o impacto da Lei 12.737/2012 e a (des)construção de uma dogmática penal dos crimes cibernéticos*. 2018. 231f. Tese (doutorado) – Universidade Federal de Pernambuco. Recife, 2018, p. 114-115. No mesmo sentido, A União Internacional de Telecomunicações também ressalta a diferença entre o crime cibernético e o "crime computadorizado". O primeiro vincula-se às condutas que atingem uma rede de computadores, enquanto o segundo diz respeito à conduta não ofensiva à rede em si, mas que faz uso dos sistemas de computadores para sua finalidade. INTERNATIONAL TELECOMMUNICATION UNION. *Understanding Cybercrime: Phenoma, challenges and legal response*. ITU: 2012, p. 11. Disponível em: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf. Acesso em 14/06/2021.

[23] SANTOS, Paulo Ernani Bergamo dos. *Direito internacional e o combate à cibercriminalidade contra crianças*. In: BRASIL. Ministério Público Federal. Crimes cibernéticos. 2ª Câmara de Coordenação e Revisão, Criminal. MPF: Brasília, 2018, p. 164. Disponível em: https://memorial.mpf.mp.br/nacional/vitrine-virtual/publicacoes/crimes-ciberneticos-coletanea-de-artigos. Acesso em 14/06/2021.

computadores são utilizados como instrumento para a prática da conduta. A terceira faz referência ao uso do computador como "um aspecto incidental da prática do crime, mas que pode trazer evidências do crime, como endereços encontrados no computador de um suspeito de assassinato"[24].

A classificação dos crimes cibernéticos em próprios e impróprios revela efeitos na política criminal, que a legislação atinente aos crimes impróprios é muitas vezes suficiente para a penalização adequada, pois já garante proteção dos bens jurídicos ofendidos. Entretanto, os próprios não possuem tipificação legal apropriada, razão pela qual o exercício da jurisdição penal era prejudicado.[25] O relatório elaborado pela EUROPOL avalia que a evolução dos crimes cibernéticos também está relacionada com a conexão a apropriação de tecnologias da informação e da comunicação para o exercício das tradicionais formas de crime – relação que representa os crimes virtuais impróprios[26].

O aumento do número de crimes virtuais revela que danos e impactos provocados no ambiente cibernético foram ampliados. Dados da Polícia Federal e da Associação Brasileira de Especialista em Alta Tecnologia, destacados por Castro, revelam que os crimes cibernéticos são os mais rentáveis no Brasil, já que apresentam maiores vantagens econômicas auferidas do que aquelas obtidas com o narcotráfico, com a possibilidade

---

[24] WANG, Qianyun. *A Comparative Study of Cybercrime in Criminal Law: China, US, England, Singapore and the Council of Europe*. Tese (doutorado) – Erasmus University Rotterdam. Rotterdam, 2016, p. 9-10. Versão original: crimes in which the use of the computer is an incidental aspect of the commission of the crime but may afford evidence of the crime, such as addresses found in the computer of a murder suspect.

[25] CASTRO, José Roberto Wanderley. *A tipicidade dos crimes cibernéticos no direito penal brasileiro: um estudo sobre o impacto da Lei 12.737/2012 e a (des)construção de uma dogmática penal dos crimes cibernéticos*. 2018. 231f. Tese (doutorado) – Universidade Federal de Pernambuco. Recife, 2018, p. 115.

[26] EUROPOL. *Internet Organized Crime Threat Assessment (IOCTA)*. European Agency for Law Enforcement Cooperation. 2020, p. 12. Disponível em: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020. Acesso em 14/06/2021.

concreta da sociedade e do Estado figurarem no polo passivo[27].

A ausência de legislação própria, com regras específicas para as condutas ilícitas na *internet*, é um atrativo para grupos e organizações criminosas migrarem suas atividades para o ambiente cibernético. No mesmo sentido, as novas formas e os novos usos das tecnologias associadas às omissões da legislação facilitam a criminalidade na *internet*[28].

É importante avaliar o impacto da criminalidade cibernética especificamente para o contexto brasileiro. O relatório "A Caminho da Era Digital no Brasil", elaborado pela OCDE (Organização para a Cooperação e Desenvolvimento Econômico), concluiu que o "Brasil tem sido alvo de ataques cada vez mais frequentes à segurança digital"[29].

Ao fazer uso de dados do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), o relatório identificou um aumento progressivo no número de incidentes. Dados provenientes de relatório da EUROPOL, de 2018, apontaram que o Brasil é um dos principais alvos de ataques cibernéticos na América Latina; e, ademais, 54% dos ataques à segurança digital no Brasil se originaram no próprio país. Esta constatação indica que possivelmente 46% dos ataques cibernéticos no Brasil possuem origem fora do nosso território, o que comprova o caráter transnacional da criminalidade que ultrapassa as tradicionais fronteiras físicas dos Estados[30].

---

[27] CASTRO, José Roberto Wanderley. *A tipicidade dos crimes cibernéticos no direito penal brasileiro: um estudo sobre o impacto da Lei 12.737/2012 e a (des)construção de uma dogmática penal dos crimes cibernéticos*. 2018. 231f. Tese (doutorado) – Universidade Federal de Pernambuco. Recife, 2018, p. 102-103.

[28] CASTRO, José Roberto Wanderley. *A tipicidade dos crimes cibernéticos no direito penal brasileiro: um estudo sobre o impacto da Lei 12.737/2012 e a (des)construção de uma dogmática penal dos crimes cibernéticos*. 2018. 231f. Tese (doutorado) – Universidade Federal de Pernambuco. Recife, 2018, p. 103.

[29] OCDE. *A Caminho da Era Digital no Brasil*. OECD Publishing: Paris, 2020, p. 108.

[30] OCDE. *A Caminho da Era Digital no Brasil*. OECD Publishing: Paris, 2020, p. 108. O relatório da OCDE também identifica, dessa vez com base em dados da LexisNexis Threatmetrix, que o Brasil é o sexto país em termos de origem de ataques

O diagnóstico presente na Estratégia Nacional de Segurança Cibernética indica que o número de ataques cibernéticos aumentou em 95,9% em 2018, quando comparado com os dados de 2017 no Brasil, conforme dados do laboratório especializado em segurança cibernética da PSafe[31].

No contexto da pandemia de COVID-19, o potencial lesivo dos crimes cibernéticos é ampliado em decorrência das políticas de isolamento social e das demais restrições sanitárias impostas, porque indivíduos e empresas passaram a trabalhar de maneira remota. Esse fenômeno implica em aumento dos fluxos de dados sensíveis de corporações entre indivíduos especialmente distantes, bem como no aumento das atividades *online*[32].

O relatório da EUROPOL também aponta o aumento da criminalidade virtual na pandemia em decorrência do incremento de informações falsas na *internet*. Dessa forma, uma vez considerado o enorme volume de informações disponíveis, os usuários estão mais vulneráveis e receptivos às informações falsas e *fake news*, e este maior contato amplia o alcance e a

cibernéticos no mundo inteiro, considerando o volume dos crimes praticados. Dados do Norton Survey indicam que, em 2017, 70,4 milhões de brasileiros foram vítimas de cibercrimes.

[31] BRASIL. *Estratégia Nacional de Segurança Cibernética*. 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm. Acesso em 21/06/2021. O diagnóstico presente na estratégia revela: Nos últimos três meses de 2018, foram registrados sessenta e três milhões e oitocentos mil *links* maliciosos, um aumento de 12% em relação ao início daquele ano, sendo campeões de golpes os *links* de aplicativos de mensagens como WhatsApp. Ao todo, 57,4% dos ataques foram realizados por meio de *phishing*, enquanto, em segundo, ficaram os golpes com publicidade suspeita, que somaram 19,2% dos casos.

[32] EUROPOL. *Internet Organized Crime Threat Assessment (IOCTA)*. European Agency for Law Enforcement Cooperation. 2020, p. 13. O relatório identifica aumento de golpes cibernéticos, na medida em que "atividades tradicionais de cibercrime como *phishing* e golpes cibernéticos rapidamente se aproveitam de vulnerabilidades sociais à medida que muitos indivíduos e negócios estavam buscando por informações, respostas e fontes de ajuda durante esse tempo" (tradução nossa). Versão original: Traditional cybercrime activities such as phishing and cyber-enabled scams quickly exploited the societal vulnerability as many citizens and business were looking for information, answers and sources of help during this time.

efetividade de golpes de *phishing* e de engenharia social[33].

Castro explica que as novas relações desenvolvidas no ciberespaço são complexas e de difícil compreensão pelos legisladores quando são demandados para elaborarem a descrição da conduta proibida pertinente. A complexidade das condutas praticadas no espaço cibernético e as mais diversas possibilidades de práticas ilícitas dificultam a tipificação penal[34].

O relatório elaborado pela EUROPOL identifica que uma das dificuldades no enfrentamento da criminalidade virtual é a falta de definição da conduta constitutiva do tipo penal. Nesse sentido, a presença de tipos penais genéricos e abertos dificultam o registro pormenorizado do crime virtual que efetivamente ocorreu[35].

No ordenamento jurídico brasileiro, ressalta-se a Lei nº 12.737 de 2012, que altera o Código Penal ao inserir a tipificação dos "delitos informáticos". A legislação inova com o tipo penal de "invasão de dispositivo informático" e altera a redação dos crimes presentes nos artigos 266 e 298 para "interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública", "falsificação de documento particular" e "falsificação de cartão"[36].

É fato que os crimes associados às tecnologias

---

[33] EUROPOL. *Internet Organized Crime Threat Assessment (IOCTA)*. European Agency for Law Enforcement Cooperation. 2020, p. 13.

[34] CASTRO, José Roberto Wanderley. *A tipicidade dos crimes cibernéticos no direito penal brasileiro: um estudo sobre o impacto da Lei 12.737/2012 e a (des)construção de uma dogmática penal dos crimes cibernéticos*. 2018. 231f. Tese (doutorado) – Universidade Federal de Pernambuco. Recife, 2018, p. 106.

[35] EUROPOL. *Internet Organized Crime Threat Assessment (IOCTA)*. European Agency for Law Enforcement Cooperation. 2020, p. 19.

[36] Artigo 154-A do Código Penal brasileiro: "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." BRASIL. *Lei nº 12.737, de 30 de novembro de 2012*. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 14/06/2021.

ultrapassam as fronteiras físicas dos Estados. Neste sentido, a sua transnacionalidade inaugura um permanente processo de expansão do Direito Penal que, certamente, transcende a ofensa da intimidade individual. Significa dizer que, o caráter transnacional e, consequentemente, o risco aqui representado, estão ligados à ideia de ofensa à informação em sua dimensão funcional. Nesta nova dimensão, a informação adquire *status* de sujeito de tutela penal e torna-se, na atualidade, significativa para o funcionamento e o desenvolvimento dos mercados mundiais. Essa valorização da informação, vinculada ao avanço incessante da tecnologia, provocou a derrubada de muitas fronteiras até então consideradas infranqueáveis.

Segundo Castro, a *internet* altera as percepções de tempo e espaço, elemento que, em relação à prática de crimes, influi diretamente na aplicação da legislação penal[37]. As distâncias perdem relativa importância e novas formas de compreender o espaço e o tempo surgem, diante da comunicação instantânea e da transferência de informações[38].

Santos destaca que mais de 50% dos crimes praticados no domínio da *internet* possui algum elemento transnacional[39]. Dessa forma, o exercício da persecução criminal muitas vezes envolve diferentes jurisdições. Por essa razão, o adequado enfrentamento dos crimes cibernéticos requer cooperação internacional e, portanto, demanda a existência de instrumentos que viabilizem o diálogo e o auxílio mútuo entre os Estados.

---

[37] CASTRO, José Roberto Wanderley. *A tipicidade dos crimes cibernéticos no direito penal brasileiro: um estudo sobre o impacto da Lei 12.737/2012 e a (des)construção de uma dogmática penal dos crimes cibernéticos*. 2018. 231f. Tese (doutorado) – Universidade Federal de Pernambuco. Recife, 2018, p. 115.

[38] BAUMAN, Zygmunt. *Globalização: As consequências humanas*. Rio de Janeiro: Zahar, 1999, p. 85-111.

[39] SANTOS, Paulo Ernani Bergamo dos. *Direito internacional e o combate à cibercriminalidade contra crianças*. In: BRASIL. Ministério Público Federal. Crimes cibernéticos. 2ª Câmara de Coordenação e Revisão, Criminal. MPF: Brasília, 2018, p. 168. Disponível em: https://memorial.mpf.mp.br/nacional/vitrine-virtual/publicacoes/crimes-ciberneticos-coletanea-de-artigos. Acesso em 14/06/2021.

O relatório da OCDE supramencionado destaca a necessidade de cooperação internacional para as novas necessidades decorrentes das inovações tecnológicas. O relatório aponta que, diante do incremento da demanda por bens e serviços na *internet* e do aumento do uso das redes sociais, a cooperação no cumprimento de leis de proteção de dados é essencial para reforçar a confiança dos consumidores[40].

Em relação à cooperação internacional em matéria penal e à internacionalização do direito cibernético, Castro destaca a importância dos trabalhos da União Europeia na conclusão da Convenção de Budapeste sobre *Cibercrime*, assinada em 2001. Nesse sentido, para além da punição e da extradição dos responsáveis pela via da assistência jurídica mútua, a Convenção viabiliza a racionalidade do Direito Penal em cooperação internacional ao destacar a importância da tipificação de condutas por meio da harmonização da legislação penal[41]. Nesse ponto, a harmonização garantirá o enfrentamento do crime ao permitir o diálogo internacional entre os diversos sistemas judiciais.

A Convenção apresenta crimes virtuais próprios a serem tipificados pela via da harmonização. Nesta direção, Castro, igualmente, aponta a importância da Convenção de Budapeste como modelo técnico a ser seguido pelos Estados ao lidarem com a criminalidade cibernética, ainda que estes não adiram efetivamente ao seu regramento[42].

A importância da Convenção para compreensão da tipificação do *cibercrime* pode ser avaliada a partir de condutas

---

[40] OCDE. *A Caminho da Era Digital no Brasil*. OECD Publishing: Paris, 2020, p. 132.

[41] CASTRO, José Roberto Wanderley. *A tipicidade dos crimes cibernéticos no direito penal brasileiro: um estudo sobre o impacto da Lei 12.737/2012 e a (des)construção de uma dogmática penal dos crimes cibernéticos*. 2018. 231f. Tese (doutorado) – Universidade Federal de Pernambuco. Recife, 2018, p. 108-111.

[42] CASTRO, José Roberto Wanderley. *A tipicidade dos crimes cibernéticos no direito penal brasileiro: um estudo sobre o impacto da Lei 12.737/2012 e a (des)construção de uma dogmática penal dos crimes cibernéticos*. 2018. 231f. Tese (doutorado) – Universidade Federal de Pernambuco. Recife, 2018, p. 108.

contra a confidencialidade, a integridade e a disponibilidade de dados e sistemas de computador, conforme abaixo:

> a) os cibercrimes, tipificando-os como infrações contra sistemas e dados informáticos (Capítulo I); b) infrações relacionadas com computadores; c) informações relacionadas com o conteúdo, pornografia infantil; e d) infrações relacionadas com a violação de direitos autorais, todos devidamente tipificados[43].

Em primeiro lugar, a necessidade de tipificar o "acesso ilegítimo" engloba ameaças ou ataques contra a segurança de sistemas ou dados de computadores, com o objetivo de clarificar a proteção dos indivíduos e organizações no uso e nas operações de seus sistemas. Segundo o relatório, o termo "acesso" deve compreender a invasão de um sistema de computador como um todo ou de uma ou mais partes deste, sem a devida autorização[44].

Outro aspecto a ser observado para a tipificação refere-se à "intercepção ilegítima." Este aspecto deve buscar consagrar juridicamente o direito à privacidade da comunicação de dados. Neste sentido, a conduta poderá envolver os verbos "escutar", "monitorar" e "vigiar" o conteúdo de comunicações, incluindo a possibilidade de gravação deste conteúdo, por meio do uso de meios tecnológicos associados ao domínio cibernético, sem a devida autorização. Mas, o crime relativo à "interferência em dados" deverá buscar proteger os sistemas e os dados de computadores contra eventuais danos, isto é, contra alterações negativas de sua integridade ou de seu conteúdo[45].

---

[43] CASTRO, José Roberto Wanderley. *A tipicidade dos crimes cibernéticos no direito penal brasileiro: um estudo sobre o impacto da Lei 12.737/2012 e a (des)construção de uma dogmática penal dos crimes cibernéticos*. 2018. 231f. Tese (doutorado) – Universidade Federal de Pernambuco. Recife, 2018, p. 121.

[44] CONSELHO DA EUROPA. *Explanatory Report to the Convention on Cybercrime*. 2001, p. 9. Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b. Acesso em: 20/06/2021.

[45] CONSELHO DA EUROPA. *Explanatory Report to the Convention on Cybercrime*. 2001, p. 10-11. Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b. Acesso em: 20/06/2021.

Já a tipificação voltada à "interferência em sistemas" prevê a criminalização de condutas prejudiciais ao adequado uso de sistemas de computadores, de modo a garantir que as pessoas possam utilizá-los em suas funções previstas. As condutas que podem prejudicar de tal maneira os sistemas de computadores incluem os verbos "adicionar", "transmitir", "prejudicar", "deletar", "alterar" ou "suprimir" dados de computadores.

Por fim, o tipo uso indevido de dispositivos está ligado ao manejo, armazenamento, compra, entre outras práticas, de determinadas ferramentas próprias para a prática de crimes cibernéticos. O *explanatory report* da Convenção entende, sobre este artigo, que o enfrentamento efetivo dos crimes virtuais exige a proibição de condutas potencialmente perigosas desde a fonte, mesmo que antecipando a prática da ofensa em si[46]. O artigo 6º da convenção, então, pode possibilitar a criminalização de atos preparatórios que compreendam as condutas dos artigos 2º, 3º, 4º e 5º, caso estes atos sejam potencialmente perigosos. Há, nesse ponto, risco de expansão do Direito Penal ao potencialmente alcançar os atos preparatórios de uma conduta criminosa.

Segundo o UNODC, a partir de uma base de dados de 200 itens de normas domésticas, menos de 5% utilizavam o termo "*cibercrime*", mas preferiam terminologias como "crimes de computador", crimes de "comunicações eletrônicas", "tecnologias da informação" ou "alta tecnologia" para incluir condutas criminosas como acesso não autorizado a sistemas de computadores. No mesmo sentido, os estudos do UNODC apontam que poucos instrumentos internacionais ou regionais definem propriamente "*cibercrime*". A Convenção de Budapeste, por exemplo, não apresenta definição própria para "*cibercrime*"[47].

---

[46] CONSELHO DA EUROPA. *Explanatory Report to the Convention on Cybercrime*. 2001, p. 12-13. Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b. Acesso em: 20/06/2021.

[47] ESCRITÓRIO DAS NAÇÕES UNIDAS SOBRE DROGAS E CRIME. *Comprehensive Study on Cybercrime*. United Nations: Viena, 2013, p. 12. Disponível:

Diante do exposto neste tópico, é possível verificar que os crimes cibernéticos foram dotados de maior proeminência nos últimos anos, possuindo forte caráter transnacional. Por essa razão, a cooperação internacional é fundamental para a adequada resposta jurisdicional a esta criminalidade. Para tanto, conforme igualmente foi analisado, é necessário haver harmonização legislativa por parte dos Estados em relação aos tipos penais próprios dos crimes virtuais.

ENTRE A HARMONIZAÇÃO LEGISLATIVA E O RECRUDESCIMENTO CRIMINAL: A EXPANSÃO DO DIREITO PENAL NO MEIO CIBERNÉTICO E A COOPERAÇÃO INTERNACIONAL

Uma vez considerado o caráter transfronteiriço dos crimes cibernéticos, conforme procurou se demonstrar no tópico anterior, destaca-se o caráter internacional que tal criminalidade assume. Vislumbra-se, igualmente, a possibilidade de várias jurisdições serem competentes para um mesmo fato. É importante, nessas hipóteses, haver critérios claros para os Estados aplicarem suas jurisdições criminais.

A cooperação internacional em matéria penal se faz necessário quando do enfrentamento da criminalidade virtual. Com a finalidade de viabilizar a adequada prestação jurisdicional, no campo da cooperação internacional, é necessário haver diálogo jurídico entre os Estados cooperantes. É necessário que as legislações criminais aplicáveis no âmbito doméstico tenham algum grau de coerência entre si. Nesse sentido, instrumentos bilaterais ou multilaterais são importantes para esclarecer os termos que vinculam os Estados.

Wang identifica que as inconsistências, isto é, a falta de harmonização normativa, entre as legislações nacionais são

---

https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf. Acesso em 14/06/2021.

dificuldades para o enfrentamento adequado da criminalidade cibernética. No domínio interno, por sua vez, a limitação da cobertura dos tipos penais tradicionais para a criminalidade virtual, bem como os conflitos de jurisdição recorrente, são elementos que tornam mais complexa a prestação jurisdicional. Outro aspecto apresentado diz respeito à natureza transitória dos cibercrimes, de modo que as rápidas transformações tecnológicas implicam em mudanças nos modos e, também, nos conceitos que circundam esta criminalidade. Por essa razão, as legislações podem se tornar mais facilmente obsoletas[48].

Em relação aos crimes virtuais, a Convenção de Budapeste de 2001 é instrumento internacional de abrangência importante para este estudo. O Brasil foi convidado pelo Comitê de Ministros do Conselho da Europa em 2019, de modo que o processo de adesão teve início em julho de 2019. Segundo a nota número 309/2019, veiculada pelo Ministério de Relações Exteriores, o Governo brasileiro manifestou intenção de aderir ao processo, contexto em que destacou a oportunidade de ampliar a efetividade da cooperação jurídica internacional em matéria penal no enfrentamento dos crimes cibernéticos. Para tanto, a nota assevera, é necessário que a legislação brasileira se adeque

[48] WANG, Qianyun. *A Comparative Study of Cybercrime in Criminal Law: China, US, England, Singapore and the Council of Europe*. Tese (doutorado) – Erasmus University Rotterdam. Rotterdam, 2016, p. 17-21. Nesse sentido, Wang assevera: [...] *cibercrime* também apresenta problemas no nível internacional. Especificamente, *cibercrimes* transfronteiriços expõem as inconsistências das leis e dos regulamentos para além das fronteiras. O *cibercrime* é national: enquanto uma ofensa, por sua natureza, trata-se de algo que as legislações nacionais devem atuar. No entanto, ele também possui consequências internacionais: o posicionamento de um país em relação ao direito cibernético ou a falta de legislações sobre o tema podem gerar impactos consideráveis em outros países (tradução nossa). Versão original: [...] cybercrime also presents problems at the international level. Namely, cross-border cybercrime manifests the inconsistencies of laws and regulations across state boundaries. Cybercrime is national: making it an offence by nature something which national legislation should govern. However, it also has international consequences: a country's position as regards cyber laws or lack of cyber laws can have a considerable impact on other countries.

às normas da Convenção de Budapeste[49].

Nesse contexto, é importante destacar o movimento de internacionalização do Direito Penal. Segundo Marcus Vinícius Xavier de Oliveira, identifica-se este processo no contexto de aproximação da atividade jurisdicional criminal dos Estados a um sistema internacional de cooperação internacional em matéria penal, seja ele de caráter universal ou regional[50].

Em razão desta compatibilização entre normas domésticas e internacionais, verificam-se novas obrigações para os Estados nesta temática: necessidade de tipificação de condutas, com o objetivo de garantir coerência dentro do sistema criminal; e o dever de cooperação judiciária e policial[51]. Ressalva-se que, ao utilizar os termos "obrigação" e "necessidade", tratam-se de conjecturas necessárias com o fim de promover a adequada cooperação internacional em matéria penal entre os Estados, todavia não são imperativos normativos internacionais que violam *a priori* a soberania dos Estados.

É possível conceber o fenômeno em duas perspectivas. A primeira se refere à progressiva transferência de competências

---

[49] BRASIL. *Processo de adesão à Convenção de Budapeste – Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública. Nota 309*. Ministério das Relações Exteriores. 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 20/06/2021.

[50] OLIVEIRA, Marcus Vinícius Xavier de. *Temas escolhidos sobre a internacionalização do direito penal*. Porto Alegre: Editora Fi, 2015, p. 44-45. Nesse sentido, Oliveira destaca: tanto a competência legislativa do estado como o exercício de seu poder persecutório em relação ao fenômeno criminal está, em graus bastante variados, vinculado50 ao sistema internacional de cooperação internacional em matéria penal, sejam eles de caráter universal através das diversas Convenções Internacionais pactuadas na ONU (para ficarmos em alguns exemplos, as Convenções onusianas sobre o Tráfico de Entorpecentes, o Crime Organizado, Contra a Corrupção e Contra o Financiamento do Terrorismo, além de, obviamente, o Estatuto de Roma e a CIPTPCDF), seja de caráter regional, no âmbito, e.g., da União Europeia e da Organização dos Estados Americanos [...].

[51] OLIVEIRA, Marcus Vinícius Xavier de. *Temas escolhidos sobre a internacionalização do direito penal*. Porto Alegre: Editora Fi, 2015, p. 44-45.

nacionais para o âmbito internacional, com maior centralidade à regulação do Direito Internacional. Nessa hipótese, a internacionalização do Direito Penal está centrada em valores comuns partilhados pelos Estados. A segunda perspectiva possível, e a essa será dada maior relevância neste trabalho, está relacionada com o aumento da regulamentação internacional pela via da cooperação multitemática entre os Estados. Em ambos os casos, exige-se dos Estados a necessidade de harmonização de suas legislações para maior alinhamento com os instrumentos internacionais, de forma a viabilizar a cooperação internacional na matéria em questão[52].

Sobre as formas de internacionalização do direito, Oliveira destaca três possibilidades: unificação, uniformização e harmonização. Em síntese, o processo de unificação corresponde ao tratamento unificado de institutos jurídicos, em conformidade com o Direito Internacional. Na sequência, a uniformização possui a finalidade de estabelecer regulamentos internos coerentes com determinado regime jurídico internacional, mas mantendo flexibilidade em relação à cultura jurídica de cada Estado. O processo de harmonização, ademais, busca assegurar harmonia entre as normas internacionais e as normas domésticas dos Estados, diante das hipóteses impossibilidade de uniformização legislativa[53].

A Convenção de Budapeste, conforme já destacado neste artigo, compreende quatro tipos de ofensas praticáveis pela criminalidade cibernética: crimes contra a confidencialidade, integridade ou disponibilidade de dados ou sistemas de computador; crimes relacionados com computadores; crimes relacionados com o conteúdo; e crimes relacionados com direitos autorais[54].

---

[52] OLIVEIRA, Marcus Vinícius Xavier de. *Temas escolhidos sobre a internacionalização do direito penal*. Porto Alegre: Editora Fi, 2015, p. 35-36.
[53] OLIVEIRA, Marcus Vinícius Xavier de. *Temas escolhidos sobre a internacionalização do direito penal*. Porto Alegre: Editora Fi, 2015, p. 38-42.
[54] CONSELHO DA EUROPA. *Convention on Cybercrime*. 2001. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185. Acesso

Há, na Convenção, importante enfoque para os crimes cibernéticos praticados contra a confidencialidade, integridade e a disponibilidade de dados ou sistemas de computador. A Convenção, nesse sentido, destaca o dever de os Estados tipificarem condutas que representam a mencionada ofensa, quais sejam acessos ilegais a sistemas de computadores, interceptação ilegal de dados, interferência em dados, interferência em sistemas e o uso indevido de dispositivos[55].

Ressalta-se, nesse sentido, a previamente exposta necessidade de harmonização vertical por parte dos países membros com vistas a viabilizar os processos de cooperação internacional em matéria penal. Os tipos penais acima elencados e anteriormente descritos representam crimes cibernéticos próprios. Dessa forma, é necessário que exista tipificação penal particular e objetiva para tais condutas.

No caso brasileiro, conforme a Nota nº 309/2020 assegurou, é necessária a adequação do ordenamento jurídico nacional com o objetivo de viabilizar a adesão à Convenção de Budapeste[56]. Entende-se, destarte, que é central para tal adesão a previsão de tipos penais próprios aos crimes virtuais, especialmente em se tratando das condutas previstas no Título 1 da Convenção. Trata-se, como mencionado, de movimento de harmonização vertical da legislação.

O Projeto de Lei nº 4554/2020, contudo, não caminha no mesmo sentido da harmonização vertical dos institutos jurídicos presentes na Convenção de Budapeste, instrumento

em: 20/06/2021.

[55] CONSELHO DA EUROPA. *Convention on Cybercrime*. 2001. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185. Acesso em: 20/06/2021.

[56] BRASIL. *Processo de adesão à Convenção de Budapeste – Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública. Nota 309*. Ministério das Relações Exteriores. 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 20/06/2021.

internacional ao qual o Brasil foi convidado a aderir. Trata-se não da criação de institutos penais próprios para se lidar com a criminalidade digital, mas da inserção de crimes já tipificados no plano físico para o domínio cibernético, com penalizações mais severas.

O Projeto de Lei nº 4554/2020, nesse sentido, torna mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica o pela internet. Segundo o explicativo da ementa, pretende-se criar o "crime de furto qualificado pela fraude com uso de dispositivo eletrônico ou de dados eletrônicos fornecidos indevidamente [...]", com previsão também de aumento de pena quando se tratar de vítima idosa ou vulnerável ou nas hipóteses de uso de servidor de rede fora do território nacional. Além deste, também cria a modalidade de estelionato mediante fraude eletrônica[57].

Conforme se observa do texto presente no referido Projeto de Lei, a pena para o furto praticado mediante fraude com uso de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programas maliciosos, corresponde a reclusão de quatro a oito anos. Ainda, há a possibilidade de a pena ser ampliada em um terço no caso a de vítima ser idosa ou vulnerável ou no caso de o crime ser praticado mediante a utilização de servidor mantido fora do território nacional[58].

Ressalva-se que, diante do paradigma do Projeto de Lei nº 4554/2020, é possível verificar tendência de recrudescimento do poder punitivo no campo digital, diante da desproporcionalidade das penas, ainda que não necessariamente buscando

[57] BRASIL. Câmara dos Deputados. *Projeto de Lei nº 4554, de 2020. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal)*. Brasília: Câmara dos Deputados, 2020. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/148159. Acesso em 21/06/2021.

[58] BRASIL. Câmara dos Deputados. *Projeto de Lei nº 4554, de 2020. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal)*. Brasília: Câmara dos Deputados, 2020. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/148159. Acesso em 21/06/2021.

harmonização necessária aos termos da Convenção de Budapeste. O aumento desproporcional de penas para crimes praticados no meio virtual reforça a percepção de incipiente formação de um Estado de polícia próprio ao ciberespaço, como forma de ampliar a presença estatal neste espaço em razão das próprias fragilidades percebidas pelo Estado contemporâneo no domínio cibernético.

Mesmo o processo de harmonização legislativa do conteúdo da Convenção de Budapeste deve ser cauteloso. O artigo 6º da Convenção, ao destacar a possibilidade de punição pela realização de atos potencialmente perigosos que antecedem a conduta criminosa constante nos artigos 2, 3, 4 e 5, indica a possibilidade de expansão do direito penal para a criminalização de atos preparatórios em relação aos crimes virtuais[59].

O ordenamento jurídico brasileiro não caminha em prol da harmonização vertical da criminalização para fins de cooperação internacional em matéria penal, com base em Budapeste, quando se considera aprovação de legislação como o Projeto de Lei nº 4554/2020. Nesse caso, na verdade, está mais próximo da construção de um Estado de Polícia, com penas mais severas, e com uma estrutura menos eficiente, com baixa tipificação dos tipos penais associados aos bens jurídicos que realmente são afetados nos crimes digitais.

Por essa razão, não oferece segurança aos bens jurídicos que efetivamente necessitam de proteção específica diante da criminalidade cibernética, ao passo que qualifica condutas do meio físico dentro do ambiente cibernético, com ampliação desproporcional da pena. Estaria, nesse sentido, apenas tornando as penas mais severas em detrimento de adequado processo de harmonização legislativa para se lidar com os crimes virtuais, como se pode verificar na Convenção de Budapeste. A mera adoção

[59] CONSELHO DA EUROPA. *Explanatory Report to the Convention on Cybercrime*. 2001, p. 12-13. Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b. Acesso em: 20/06/2021.

de penas mais severas não contribui para a harmonização legislativa que é necessária à cooperação internacional – cooperação está que é fundamental para o enfrentamento cibercriminalidade, uma vez considerado o caráter transfronteiriço de tais crimes.

O lançamento da Estratégia Nacional de Segurança Cibernética, em 2020, permite identificar as intenções, os diagnósticos e os planos de ação da política governamental para o enfrentamento da criminalidade virtual. Nesta, destaca-se o tratamento relativo à cooperação internacional para lidar com a temática.

Inicialmente, o documento mencionado define "segurança digital" como a "gestão de riscos econômicos e sociais resultantes de violações em relação à disponibilidade, integridade, e confidencialidade de hardware, software, redes e dados"[60].

Os objetivos estratégicos apresentados na Estratégia possuem a finalidade de ampliar o horizonte de segurança cibernética do Brasil, levando em consideração as necessidades e possibilidades do país. São objetivos destacados: "1. tornar o Brasil mais próspero e confiável no ambiente digital; 2. Aumentar a resiliência brasileira às ameaças cibernéticas; e 3. Fortalecer a atuação brasileira em segurança cibernética no cenário internacional"[61].

No item 2.3.6 da Estratégia, destaca-se a necessidade de aprimorar o arcabouço legal sobre a segurança cibernética. O texto cita como ação estratégica a revisão e atualização da legislação aplicável, incluindo a possiblidade de se abordar novas temáticas e de elaborar novos instrumentos. Nesse ponto, recomenda a identificação de temas ausentes na legislação vigente. O programa destaca, igualmente, que a elaboração de lei sobre segurança cibernética poderia alinhar ações de governança e de

[60] OCDE. *A Caminho da Era Digital no Brasil*. OECD Publishing: Paris, 2020, p. 109.
[61] BRASIL. *Estratégia Nacional de Segurança Cibernética*. 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm. Acesso em 21/06/2021.

conformidade, melhor adaptando o ordenamento jurídico brasileiro para o tratamento do tema[62].

No ponto 2.3.8, a Estratégia trata da ação estratégica "Ampliar a cooperação internacional do Brasil em Segurança cibernética". Nesta, o documento recomenda:

> Estimular a cooperação internacional em segurança cibernética; incentivar as discussões sobre segurança cibernética nos organismos, nos fóruns e nos grupos internacionais dos quais o Brasil é membro; ampliar o relacionamento internacional com os países da América Latina; promover eventos e exercícios internacionais sobre segurança cibernética; participar de eventos internacionais de interesse para o País; ampliar os acordos de cooperação em segurança cibernética; ampliar o uso de mecanismos internacionais de combate aos crimes cibernéticos; estimular a participação do País em iniciativas futuras de estruturação normativa, como as relativas à criação de padrões de segurança em tecnologias emergentes, e identificar, estimular e aproveitar novas oportunidades comerciais em segurança cibernética[63].

Em relação ao eixo temático "Dimensão Internacional e Parcerias Estratégicas", o documento reconhece a necessidade de cooperação internacional para o enfrentamento da criminalidade cibernética e recomenda o reforço da participação brasileira na elaboração e na revisão dos instrumentos internacionais concernentes. O texto defende a busca por acordos bilaterais neste tema, com o objetivo de ampliar as parcerias estratégias, e recomenda, igualmente, a criação de canais apropriados para o diálogo sobre a temática. Contudo, embora realce a ênfase ao multilateralismo na orientação da cooperação internacional, o texto não avança nessa temática e tampouco trata da Convenção de Budapeste[64].

---

[62] BRASIL. *Estratégia Nacional de Segurança Cibernética*. 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm. Acesso em 21/06/2021.

[63] BRASIL. *Estratégia Nacional de Segurança Cibernética*. 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm. Acesso em 21/06/2021.

[64] BRASIL. *Estratégia Nacional de Segurança Cibernética*. 2020. Disponível em:

Verifica-se, segundo relatório da OCDE, percepção de que o governo brasileiro está alçando maior valor à segurança cibernética, incluindo-a como setor prioritário para a economia e para a sociedade. No entanto, "a maior parte dos atores públicos e privados não está dando atenção e recursos suficientes a essa questão".[65] Adiante, aponta o relatório que os documentos legais no Brasil utilizam terminologias distintas quando tratam da temática de segurança cibernética, de modo que as definições adotadas não sejam dotadas de consistência ao longo do tempo[66].

Diante do exposto, verifica-se que, malgrado a Estratégia Nacional de Segurança Cibernética busque apresentar visão global da criminalidade virtual e incentive estratégias multitemáticas, englobando atores públicos e privados, nacionais e

http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm. Acesso em 21/06/2021.

[65] OCDE. *A Caminho da Era Digital no Brasil*. OECD Publishing: Paris, 2020, p. 118-119. Sobre a evolução da preocupação do governo brasileiro com a segurança cibernética, destaca-se: The institutionalization of cybersecurity in Brazil was catalyzed by two main events. The first was the approval of the Marco Civil da Internet (the Digital Bill of Rights) in 2013, motivated by the political impact of the revelations regarding the United States' virtual surveillance structure. The second was a direct consequence of the mega-events hosted by the country between 2012 and 2016, which included efforts such as (i) the creation of the Cyber Defense Center (CDCiber); (ii) cybersecurity capacity building efforts by public institutions on the federal and municipal levels; (iii) the increased collaboration between the government and private sector; and (iv) the establishment of doctrines, policies, and directives related to cybersecurity. HUREL, L. M.; LOBATO, L. Cruz. *A Strategy for Cybersecurity Governance in Brazil. Strategic Note 30*. Instituto Igarapé: Rio de Janeiro, 2018, p. 3. Disponível em: https://igarape.org.br/wp-content/uploads/2019/01/A-Strategy-for-Cybersecurity-Governance-in-Brazil.pdf. Acesso em 14/06/2021.

[66] OCDE. *A Caminho da Era Digital no Brasil*. OECD Publishing: Paris, 2020, p. 119-120. Ressalta-se, igualmente, a investigação do relatório da OCDE: O foco das políticas de segurança digital no Brasil evoluiu de uma dimensão técnica de 2000-11, para uma dimensão de segurança nacional de 2012-18, impulsionado em parte pela organização de megaeventos e pelas revelações de Edward Snowden sobre a espionagem cibernética dos Estados Unidos. A missão abrangente da Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética na Administração Pública Federal 2015-2018, que tinha por objetivo "assegurar e defender os interesses do estado e da sociedade para a preservação da soberania nacional", ilustra essa evolução. OCDE. *A Caminho da Era Digital no Brasil*. OECD Publishing: Paris, 2020, p. 118.

estrangeiros, bem como entidades internacionais, o Projeto de Lei nº 4554 de 2020 não caminha no mesmo sentido.

No contexto da sociedade de risco, apresentada por Ulrich Beck e previamente mencionada neste trabalho, o aumento dos riscos e, portanto, das inseguranças no meio social, há tendência de aumento da presença do Estado em ambientes onde até então não ocupava. A impossibilidade de se prever as diversas possibilidades de ameaças amplificam os riscos e o sentimento de insegurança[67]. O *cibercrime*, nesse sentido, é classificado como um forte produtor de insegurança na sociedade contemporânea, cada vez mais digitalizada e presente no meio cibernético.

Sobre a hipótese de expansão do Direito Penal e da possibilidade de emergência do Estado de Polícia em relação aos crimes cibernéticos, é importante resgatar as contribuições de Jesús-María Silva Sánchez. Segundo o autor, a sociedade de risco ou de insegurança, cujas características foram apresentadas no início deste artigo, favorece a instituição de um "Estado vigilante"[68].

Nesta sociedade, conforme aponta José Luis Díez Ripollés, há um forte sentimento de insegurança, motivado, entre outros motivos, pelos rápidos avanços tecnológicos que transformam as relações sociais e, ao mesmo tempo, pela percepção dos indivíduos de que a sociedade moderna não mais compartilha dos mesmos valores. Este sentimento incentiva, por parte da sociedade, pedidos de aumento da intervenção socioestatal, incluindo pela via da política criminal, para reduzir os níveis de insegurança[69].

---

[67] BECK, Ulrich. *La sociedad del riesgo: Hacia una nueva modernidad*. Barcelona: Paidós Ibérica, 2006, p. 237-240.

[68] SILVA SÁNCHEZ, Jesús-María. *A expansão do direito penal: aspectos da política criminal nas sociedades pós-industriais*. São Paulo: Revista dos Tribunais, 2002, p. 138.

[69] DÍEZ RIPOLLÉS, José Luis. *De la sociedad del riesgo a la seguridad ciudadana: Un debate desenfocado*. In: MELIÁ, M.C.; DÍEZ, Gómez-Jara. Derecho Penal del Enemigo: El discurso penal de la exclusión. Vol. 1. São Paulo: Livraria dos

De maneira similar, Zygmunt Bauman destaca que medidas como o processo de elaboração de novos estatutos criminais, com ampliação dos crimes puníveis com prisão, e o incremento das penas previstas para crimes, no contexto da sociedade contemporânea, aumentam a popularidade dos governos. Trata-se de movimento que contribui para formar a imagem de um governo capacitado para solucionar os conflitos e problemas desta sociedade.[70] Trata-se de processo com algum nível de coerência quando se considera, novamente segundo Bauman, em outra obra, que as autoridades estatais estão sendo contestadas progressivamente[71].

Segundo Díez Ripollés, o Direito Penal desta nova política criminal pode ser caracterizado pelos seguintes aspectos: surgimento de novos bens jurídicos de natureza coletiva, fato que ensejaria em expansão da criminalização para novas condutas; tipificação de crimes que exigem mera conduta, sem exigência de resultado material danoso; antecipação dos procedimentos de intervenção penal; flexibilização das regras e garantias do sistema de imputação da responsabilidade criminal, de forma a admitir tipos penais em branco que englobam um grande campo de condutas possíveis[72].

A expansão do Direito Penal, com o objetivo apresentar resposta adequada, nesse sentido, é necessária para fins de harmonização legislativa, isto é, para oferecer tratamento aos novos bens jurídicos lesados pela criminalidade virtual. É movimento essencial para a cooperação internacional em matéria penal. Por este ponto de vista, não se trata de emergência de um Estado de Polícia, mas de adaptação necessária às inovações tecnológicas.

advogados, 2006, p. 556-594.

[70] BAUMAN, Zygmunt. *Globalização: As consequências humanas*. Rio de Janeiro: Zahar. 1999, p. 111-137.

[71] BAUMAN, Zygmunt. *Ética pós-moderna*. São Paulo: Paulus, 1997, p. 35.

[72] DÍEZ RIPOLLÉS, José Luis. *De la sociedad del riesgo a la seguridad ciudadana: Un debate desenfocado*. In: MELIÁ, M.C.; DÍEZ, Gómez-Jara. Derecho Penal del Enemigo: El discurso penal de la exclusión. Vol. 1. São Paulo: Livraria dos advogados, 2006, p. 556-594.

Conclui-se, destarte, que a tipificação de novos tipos legais em conformidade com o processo de adesão à Convenção de Budapeste tem potencial de expandir o Direito Penal.

Todavia, o mero recrudescimento da legislação criminal já existente, com aumento das penas e sem se atentar para os novos tipos penais, permitindo a criminalização abstrata de condutas, indica movimento rumo a um Direito Penal ainda mais severo e totalizante, o que pode ser associado a um Estado de Polícia.

CONCLUSÃO

Neste artigo, propôs-se investigar a possibilidade de expansão do Direito Penal a partir do processo de harmonização legislativa para adesão à Convenção de Budapeste. Considerou-se este fenômeno uma possibilidade em razão da identificação do *cibercrime* como um risco produtor de inseguranças no contexto da sociedade de risco. Dessa forma, a emergência de novos bens jurídicos e de novas possibilidades de condutas criminosas demanda tipificação penal clara e objetiva.

A criminalidade cibernética, por ter natureza transnacional e envolver, frequentemente, agentes de diversas localizações do planeta, demanda dos Estados respostas penais mediante cooperação internacional. É necessário haver uma política criminal comum entre os Estados e a Convenção de Budapeste inaugura os parâmetros básicos para tanto

Verificou-se, ainda, que a emergência da criminalidade cibernética enseja a criação de novos tipos penais, em especial para os denominados crimes virtuais próprios. Trata-se, nesse sentido, de expansão do direito penal mediante incremento dos bens jurídicos a serem tutelados pelo Estado por meio da legislação criminal.

Contudo, a ampliação dos tipos penais, quando realizada de maneira técnica e precisa, com o objetivo de melhor regular

as atividades realizadas no meio cibernético, bem como para aproximar o ordenamento jurídico brasileiro do sistema de cooperação internacional da Convenção de Budapeste, não deve ser compreendida como ameaça aos direitos humanos e ao Estado Democrático de Direito.

Embora a evolução das tecnologias da informação e da comunicação abra oportunidades sem precedentes à humanidade, também coloca desafios, nomeadamente na esfera da justiça penal. Assim, essa nova forma de criminalidade associada à tecnologia impõe, em primeiro lugar, um autêntico desafio ao definir a informação como novo paradigma do Direito Penal em cooperação internacional. Impõe-se ressaltar que o problema da criminalização de novas condutas não reside na eleição da "segurança informática", senão sobretudo, na forma ou na técnica para a antecipação da tutela punitiva ou dos limites de proteção do bem jurídico.

Não se deve olvidar que os movimentos legislativos não estão alinhados necessariamente com essa intenção. Na verdade, conforme se verificou a partir do Projeto de Lei 4554/2020, há preocupação em intensificar as penas para crimes virtuais impróprios em detrimento de empregar esforços para a adequada abrangência legislativa para os novos tipos penais associados aos crimes virtuais próprios.

Desse modo, por um lado, a expansão do Direito Penal, com a finalidade de instituir novos tipos para abarcar as inovações tecnológicas que viabilizam criminalidade virtual, é uma necessidade para adequação ao modelo de cooperação internacional em matéria penal da Convenção de Budapeste. Por outro, todavia, o mero recrudescimento das penas para os crimes tradicionais praticados pela via digital representa preocupante ampliação do Direito Penal, uma vez que estabelece penas mais severas e não torna a legislação criminal aplicável mais precisa para a contenção da criminalidade cibernética.

Portanto, responde-se o problema proposto neste artigo

confirmando a hipótese prevista: a tipificação de novos tipos legais mediante o processo de harmonização da legislação penal produz expansão do Direito Penal. Trata-se de processo, conforme se evidenciou, associado aos estímulos da política criminal fundamentada no risco representado pelo *cibercrime*, a qual demanda ampliação dos tipos penais para englobar os novos bens jurídicos.

REFERÊNCIAS

BAUMAN, Zygmunt. *Ética pós-moderna*. São Paulo: Paulus, 1997.

BAUMAN, Zygmunt. *Globalização*: As consequências humanas. Rio de Janeiro: Zahar. 1999.

BECK, Ulrich. *La sociedad del riesgo*: Hacia una nueva modernidad. Barcelona: Paidós Ibérica, 2006.

BRASIL. *Estratégia Nacional de Segurança Cibernética*. 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm. Acesso em 21/06/2021.

BRASIL. *Processo de adesão à Convenção de Budapeste – Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública*. Nota 309. Ministério das Relações Exteriores. 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 20/06/2021.

BRASIL. Câmara dos Deputados. *Projeto de Lei nº 4554, de 2020*. Altera o Decreto-Lei nº 2.848, de 7 de dezembro

de 1940 (Código Penal). Brasília: Câmara dos Deputados, 2020. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/148159. Acesso em 21/06/2021.

BRASIL. *Lei nº 12.737, de 30 de novembro de 2012*. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 14/06/2021.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018.* Lei Geral de Proteção de Dados Pessoais (LGPD). 2018. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 14/06/2021.

CASTRO, José Roberto Wanderley. *A tipicidade dos crimes cibernéticos no direito penal brasileiro: um estudo sobre o impacto da Lei 12.737/2012 e a (des)construção de uma dogmática penal dos crimes cibernéticos*. 2018. 231f. Tese (doutorado) – Universidade Federal de Pernambuco. Recife, 2018.

CONSELHO DA EUROPA. *Convention on Cybercrime*. 2001. Disponível em: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185. Acesso em: 20/06/2021.

CONSELHO DA EUROPA. *Explanatory Report to the Convention on Cybercrime*. 2001. Disponível em: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b. Acesso em: 20/06/2021.

DÍEZ RIPOLLÉS, José Luis. *De la sociedad del riesgo a la seguridad ciudadana*: Un debate desenfocado. In: MELIÁ, M.C.; DÍEZ, Gómez-Jara. Derecho Penal del Enemigo: El discurso penal de la exclusión. Vol. 1. São Paulo: Livraria dos advogados, 2006.

ESCRITÓRIO DAS NAÇÕES UNIDAS SOBRE DROGAS E CRIME. *Comprehensive Study on Cybercrime*. United

Nations: Viena, 2013. Disponível: https://www.unodc.org/documents/organized-crime/cybercrime/CYBER-CRIME_STUDY_210213.pdf. Acesso em 14/06/2021.

EUROPOL. *Internet Organized Crime Threat Assessment* (IOCTA). European Agency for Law Enforcement Co-operation. 2020. Disponível em: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020. Acesso em 14/06/2021.

GOMES, Luiz Flávio *et al*. *Direito Penal - introdução e princípios fundamentais.* V. 1. São Paulo: Revista dos Tribunais, 2007.

HOBSBAWN, Eric. *Globalização, democracia e terrorismo*. Tradução José Viegas. São Paulo: Companhia das letras, 2007.

HUREL, L. M.; LOBATO, L. Cruz. *A Strategy for Cybersecurity Governance in Brazil*. Strategic Note 30. Instituto Igarapé: Rio de Janeiro, 2018. Disponível em: https://igarape.org.br/wp-content/uploads/2019/01/A-Strategy-for-Cybersecurity-Governance-in-Brazil.pdf. Acesso em 14/06/2021

INTERNATIONAL TELECOMMUNICATION UNION. *Understanding Cybercrime*: Phenoma, challenges and legal responde. ITU: 2012. Disponível em: https://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf. Acesso em 14/06/2021.

OLIVEIRA, Marcus Vinícius Xavier de. *Temas escolhidos sobre a internacionalização do direito penal*. Porto Alegre: Editora Fi, 2015.

OCDE. *A Caminho da Era Digital no Brasil*. OECD Publishing: Paris, 2020.

SANTOS, Boaventura de Sousa. *A globalização e as ciências*

sociais. São Paulo: Cortez. 2002.

SANTOS, Paulo Ernani Bergamo dos. *Direito internacional e o combate à cibercriminalidade contra crianças*. In: BRASIL. Ministério Público Federal. Crimes cibernéticos. 2ª Câmara de Coordenação e Revisão, Criminal. MPF: Brasília, 2018. Disponível em: https://memorial.mpf.mp.br/nacional/vitrine-virtual/publicacoes/crimes-ciberneticos-coletanea-de-artigos. Acesso em 14/06/2021.

SILVA SÁNCHEZ, Jesús-María. *A expansão do direito penal*: aspectos da política criminal nas sociedades pós-industriais. São Paulo: Revista dos Tribunais, 2002.

WANG, Qianyun. *A Comparative Study of Cybercrime in Criminal Law*: China, US, England, Singapore and the Council of Europe. Tese (doutorado) – Erasmus University Rotterdam. Rotterdam, 2016.