CRIMES VIRTUAIS: UMA ABORDAGEM JURÍDICA SOBRE OS CRIMES CIBERNÉTICOS E SEUS MECANISMOS DE PREVENÇÃO

Edílson Campelo Alexandre Júnior[1]
Volny Costa do Nascimento[2]
Franklin Vieira dos Santos[3]

Resumo: Os crimes cibernéticos são definidos como as atividades criminosas realizadas por meio do uso de dispositivos digitais, como computadores, pela Internet. Atualmente, informações são riqueza e também para ganhar dinheiro de maneira ilegal, ataques cibernéticos estão acontecendo e dados são roubados dos servidores ou dinheiro é roubado de maneira ilegal. Este artigo explora as questões legais criadas pelo uso da tecnologia de computador para cometer crimes de vários tipos, a saber, os crimes virtuais, trazendo uma abordagem jurídica sobre o tema e os seus mecanismos de prevenção. O objetivo do estudo foi realizar uma abordagem jurídica sobre os crimes virtuais no âmbito do Direito Penal brasileiro, utilizando para tanto uma abordagem bibliográfica.

Palavras-chaves: Crimes virtuais. Crimes cibernéticos. Direito Penal. Prevenção.

VIRTUAL CRIMES: A LEGAL APPROACH TO CYBER CRIMES AND THEIR PREVENTION MECHANISMES

Abstract: Cyber crimes are defined as criminal activities carried out through the use of digital devices, such as computers, over the Internet. Currently, information is wealth and also to make money illegally, cyber attacks are happening and data is stolen from servers or money is stolen illegally. This article explores the legal issues created by the use of computer technology to commit crimes of various types, namely, virtual crimes, bringing a legal approach to the subject and its prevention mechanisms. The objective of the study was to carry out a legal approach on cyber crimes in the scope of Brazilian Criminal Law, using a bibliographic approach.

Keywords: Virtual crimes. Cyber crimes. Criminal Law. Prevention.

[1]Acadêmico de Direito da Faculdade São Lucas. E-mail: alexandrejunior_pvh_@hotmail.com
[2]Acadêmico de Direito da Faculdade São Lucas. E-mail: volny_costa@hotmail.com
[3]Orientador. Juiz de Direito, Professor Universitário São Lucas, Doutor e Mestre em Direito. E-mail: franklin.santos@saolucas.edu.br

INTRODUÇÃO

A Internet, computadores, telefones celulares e outras formas de tecnologia revolucionaram todos os aspectos da vida humana nas últimas décadas, incluindo a forma como nos comunicamos, depositamos, compramos, obtemos as notícias e nos divertimos. Esses avanços tecnológicos também criaram inúmeras oportunidades para os infratores cometerem várias formas de crime. Os crimes *on-line* costumam ser chamados de cibercrime e ocorrem porque o autor usa conhecimento especial do ciberespaço. Portanto, o cibercrime pode ser visto como um grande termo abrangente que engloba crime assistido por computador no qual computadores e tecnologia são usados em uma função de suporte, como o uso de um computador para enviar mensagens de assédio. Ao mesmo tempo, o termo crime cibernético também inclui crimes focados no computador que são um resultado direto da tecnologia da computação e não existiriam sem ela, como invasão não autorizada de sistemas de computadores.

A tecnologia tem sido um grande passaporte para o crescimento e desenvolvimento de muitas pessoas, especialmente crianças no mundo. Houve muitas criações diferentes ao longo dos anos. Por exemplo, *laptops*, telefones celulares, relógios, *tablets* etc. Todos esses dispositivos tecnológicos são úteis em algum momento, com exceção de algumas crianças que não levam em consideração a responsabilidade ou o risco que podem enfrentar. Não apenas as crianças podem estar em risco de crimes virtuais, mas principalmente os adultos, já que a maioria grava suas informações pessoais em seu banco ou simplesmente usa seus cartões pessoais para comprar *on-line*. Existem diferentes responsabilidades que as pessoas devem assumir e levar em consideração que tudo pode acontecer.

Na era tecnológica, informações são consideradas como patrimônio, também utilizadas para ganhar dinheiro de maneira ilícita, ataques cibernéticos ocorrem diariamente e dados são subtraídos dos cidadãos. Crimes cibernéticos são definidos como as atividades criminosas realizadas por meio do uso de dispositivos digitais como computadores, pela Internet. Basicamente um crime cometido usando a Internet e chamado de crime cibernético. Considerando tais aspectos, a pesquisa

buscou trazer resposta ao seguinte questionamento: a estrutura e mecanismos de prevenção adotados aos crimes virtuais no Direito Penal Brasileiro são suficientes para o enfretamento destes crimes no país?

Partiu-se da hipótese que os crimes virtuais são “atividades ilegais realizadas mediante o uso da tecnologia, com objetivo de acessar ou comprometer sistemas computacionais” (GARCIA et al., 2018p. 116), e inclui o crime em que o computador está envolvido em algum formato. A Internet agiu como uma via alternativa para os criminosos conduzirem suas atividades e iniciar ataques com relativa obscuridade. Nesta época, os cibercriminosos estão identificando as redes sociais e profissionais e as ameaças são direcionadas à plataforma móvel, como smartphones e tablets. No Brasil, a Lei nº 12.737/2012 (Lei Carolina Dieckmann) possibilitou avanços no combate aos crimes virtuais, entretanto a legislação é insuficiente para combater a criminalidade virtual, visto ser um campo em constante evolução.

O objetivo geral do estudo foi realizar uma abordagem jurídica sobre os crimes virtuais no âmbito do Direito Penal brasileiro e, como objetivos específicos, buscou analisar a estrutura e mecanismo de combate aos crimes cibernéticos no sistema penal brasileiro; e verificar no Âmbito do direito penal brasileiro como ocorre o acesso á justiça e se as penas aplicadas aos crimes cibernéticos contribuem para minimizar a prática criminosa no país.

A pesquisa realizada para a elaboração deste Artigo é exclusivamente bibliográfica e descritiva. Através da legislação existente, da doutrina e da jurisprudência colacionada no Superior Tribunal de Justiça buscamos os caminhos e as orientações que deveríamos seguir. Foi utilizado como fonte de pesquisa obras editoradas e textos disponíveis na rede internacional de computadores, procuramos canalizar o pensamento dos diversos doutrinadores pesquisados, com o fim de mostrar os pontos relevantes e contraditórios dos crimes virtuais no âmbito do Direito Penal brasileiro.

1 CRIMES VIRTUAIS

Crime, no âmbito do Direito Penal brasileiro, é toda conduta típica, antijurídica e culpável (NUCCI, 2015). Crimes cibernéticos são condutas ilegais praticadas por criminoso usando um equipamento eletrônico (computador, redes de computadores ou outra forma de TIC). Esses atos incluem a disseminação de vírus e outros softwares maliciosos, *hackers* e ataques de negação de serviço distribuída (DDoS), ou seja, a inundação de servidores da Internet para derrubar a infraestrutura de rede ou sites, além de possuir o intuito de permitir a prática da conduta criminosa, conforme estabelecido no § 1º do Art. 154-A do Código Penal Brasileiro (BORTOT, 2017).

1.1 Evolução Histórica

A era dos computadores modernos começou com o mecanismo analítico de Charles Babbage. Em 1820, Joseph-Marie Jacquard, um fabricante de têxteis na França, produziu o tear. Este dispositivo permitiu a repetição de uma série de etapas na tecelagem de tecidos especiais. Isso resultou em um medo entre os funcionários de Jacquard de que seu emprego e sustento tradicionais estavam sendo ameaçados. Eles cometeram atos de sabotagem para desencorajar Jacquard do uso posterior da nova tecnologia. Este é o primeiro crime cibernético registrado (BORTOT, 2017).

Os computadores foram evoluindo nas décadas seguintes, até chegar na atual era digital, antes equipamentos gigantescos que preenchiam uma sala tiveram sua dimensão reduzida, assim como os periféricos foram diminuindo. A internet também foi outra grande evolução, hoje operam muitas redes sem fio. A maioria dos hackers estava motivada a usar dispositivos de comunicação sem fio, baixo custo e velocidade, juntamente com sistemas de computadores móveis para conexões de acesso remoto (FERREIRA, 2011).

No ano de 1966, um banco de Minnesota foi assaltado por criminosos cibernéticos usando a nova tecnologia da informação. No ano de 1969, dois funcionários do Laboratório Bell desenvolveram um novo sistema operacional chamado UNIX. O UNIX era uma maneira de invadir usando novas tecnologias. Esses dois funcionários eram Dennis Ritchie e Kene Thompson. No entanto, Stewart

Nelson foi um dos *phreakers* que descobriu o processo de uso do computador do MIT para gerar tons de telefone com a intenção de acessar serviços de longa distância das empresas de telefonia. Alguns *phreakers* usaram o processo de assobiar caixa azul para reproduzir a frequência de 2600 Hz. No ano de 1970, o mundo cibernético e a rede estavam abertos a usuários em todo o mundo. E nessa época outro crime cibernético evoluiu e se tornou um desafio legal em todo o mundo, que é a pornografia cibernética (BARRETO et al., 2020, p. 59).

1.2 Classificação dos Crimes Virtuais

Os crimes cibernéticos podem ser classificados em diferentes categorias, incluindo invasão cibernética (por exemplo, acesso não autorizado ao sistema), fraude cibernética/roubo (por exemplo, roubo de identidade, fraude online, pirataria digital), pornografia cibernética/obscenidade (por exemplo, materiais de exploração sexual infantil) e ciber-violência (por exemplo, *cyberstalking*; ciberterrorismo) (BORTOT, 2017).

De acordo com Otoboni et al. (2019, p. 54) os crimes cibernéticos podem ser classificados como próprios, impróprios, mistos e mediato ou indireto:

> 1. **Próprios**: são aqueles em que a inviolabilidade das informações automatizadas (dados) é protegida pelo bem jurídico da norma penal. O maior exemplo a ser citado nesse aspecto de crime cibernético é a invasão dos criminosos no aparelho eletrônico das vítimas;
> 2. **Impróprios**: são aqueles em que o principal aparato para sua que seja consumada a sua execução é o próprio computador, entretanto, não há que se falar em agravo ao bem jurídico estabelecido dos dados dos usuários. Exemplo: crimes contra a honra, sendo cometidos através do envio de um e-mail;
> 3. **Mistos**: são aqueles decorrentes da invasão de aparelhos eletrônicos. “Ganharam status de crimes *sui generis*, cedida a importância do bem jurídico diverso da inviolabilidade dos dados informáticos dos usuários” (VIANNA; MACHADO, 2013, p. 34).
> 4. **Mediatos ou indiretos**: são aqueles delito-fim não informático que herdou as características do delito-meio informático, realizado para configurar a própria consumação do ato em si (VIANNA; MACHADO, 2013, p. 35).

É quase impossível estimar a quantidade de crimes cibernéticos que ocorre na maioria dos países devido à falta de definições legais padronizadas para esses crimes e a poucas estatísticas oficiais válidas e confiáveis (BORTOT, 2017).

De acordo com Diniz et al., (2014, p. 9), um tratamento de amplo espectro de ameaças cibernéticas é fundamental para começar a superar concepções errôneas e abordar políticas equivocadas. Devido à novidade e à natureza técnica da questão, governos e cidadãos estão relativamente mal informados sobre como responder. Cidadãos, empresas e instituições muitas vezes acham que entender as questões está além de sua capacidade ou que as ameaças não são relevantes para eles. A ignorância ou as percepções erradas geralmente resultam em uma falha ao abordar as ameaças à segurança cibernética diretamente. As estratégias, se forem adotadas, tendem a ser remendadas com base em premissas espúrias e não testadas. Raramente existem dados robustos para orientar a tomada de decisões. Uma abordagem mais baseada em evidências é urgentemente necessária para avaliar as ameaças cibernéticas - uma abordagem informada pelo conhecimento dos numerosos e interconectados riscos online. Infelizmente, o tempo e os recursos já escassos são frequentemente alocados para áreas menos importantes, em vez de ameaças primárias reais.

No Quadro 1, Diniz et al., (2014, p. 9-10) considera o crime cibernético convencional, crimes cibernéticos complexos e ameaças emergentes para auxiliar em relação às respostas usuais dos governos e a realidade existente no Brasil.

Quadro 1. Os três principais conjuntos de ameaças cibernéticas no Brasil

Categoria	**Definição**	**Exemplos**	**Respostas usuais do governo**	**Realidade brasileira**
Cibercrime convencional	Estas são as formas de crimes cibernéticos mais difundidas no mundo e seguem a tipologia proposta pela ITU (2009)	*Acesso* ilegal (*cracking*), interceptação de dados, pornografia infantil, spam, discurso de ódio, fraude bancária, roubo de identidade, violações de direitos autorais	Exclusivamente para aplicação da lei, uma vez que normalmente abrange crimes tradicionais que já estão categorizados em códigos criminais.	Existem dois subconjuntos principais: 1) economicamente motivado (especialmente fraude bancária) e 2) relacionado ao conteúdo (por exemplo, racismo e pornografia infantil em redes de mídia social)
Cibercrime complexo	Considera e expande a definição da ITU de crimes cibernéticos	Ciberterrorismo, ciberguerra, ataques contra infraestruturas críticas,	Uma mistura de inteligência, forças armadas e policiais, já que	A espionagem comercial e o *hacktivismo* são duas ameaças, embora

	complexos ou combinados, aqueles que podem se enquadrar em mais de uma categoria de crime cibernético convencional.	ciberespionagem e *hacktivismo*	existem várias e distintas fontes potenciais de ataques (tanto internas quanto externas), bem como alvos.	distintas. Existem poucas evidências de que o Brasil seja afetado por outros tipos de ameaças desta categoria.
Ameaças emergentes	Ameaças relacionadas à expansão do ciberespaço que não se enquadram bem nas categorias da UIT, seja por serem emergentes ou mais relacionadas ao mundo em desenvolvimento.	TICs usadas por grupos criminosos mais tradicionais, como gangues e crime organizado (tráfico de drogas e armas, extorsão online, disseminação de uma cultura de violência), lavagem de dinheiro cibernética e evasão fiscal, etc.	Deveria estar mais ligado à aplicação da lei, mas este campo está apenas emergindo e ainda não há resposta do Estado.	O Brasil sofre com altos níveis de violência interpessoal e organizada, especialmente relacionada a gangues e ao crime organizado que lucram com o tráfico de drogas. Eles já aprenderam o poder das TICs para expandir e fortalecer seus negócios.

Fonte: Diniz et al., 2014, p. 9-10.

Um exemplo de crime cibernético envolve o Egghead.com. O presidente da Egghead.com, Inc., Jeff Sheahan, enviou um e-mail para vários clientes e seus emissores de cartão de crédito, notificando-os sobre um ataque ao sistema de computador da empresa. Após uma investigação do FBI e trabalho adicional por uma empresa de segurança forense (contratada pela Egghead), a Egghead.com concluiu que o sistema de segurança da empresa aparentemente interrompeu a intrusão em andamento. A evidência inicial indicou que vários milhares de contas de cartão de crédito no sistema podem ter sido afetadas.

Em geral, os crimes cibernéticos são as contrapartes modernas do crime antigo. Por exemplo, antes da era eletrônica, os vigaristas iam de porta em porta e usavam a comunicação verbal para ganhar a confiança de suas vítimas. Hoje, os criminosos contemporâneos usam a Internet e as comunicações online para perpetrar seus crimes.

O vírus de computador é o tipo de crime cibernético mais conhecido. Um vírus de computador é um programa de computador que se junta a programas aplicativos ou outro software de sistema executável; o vírus é ativado posteriormente, às vezes causando sérios danos aos sistemas ou arquivos do computador. O perpetrador não pode roubar bens, mas em vez disso, cria confusão dentro do sistema de computador da vítima.

O *phishing* é um crime cibernético que ocorre quando o perpetrador envia e-mails fictícios a indivíduos com links para sites fraudulentos que parecem oficiais e

fazem com que a vítima divulgue informações pessoais ao perpetrador. Essas informações são então usadas para fins não autorizados, como compras fraudulentas, obtenção de empréstimos fraudulentos ou roubo de identidade.

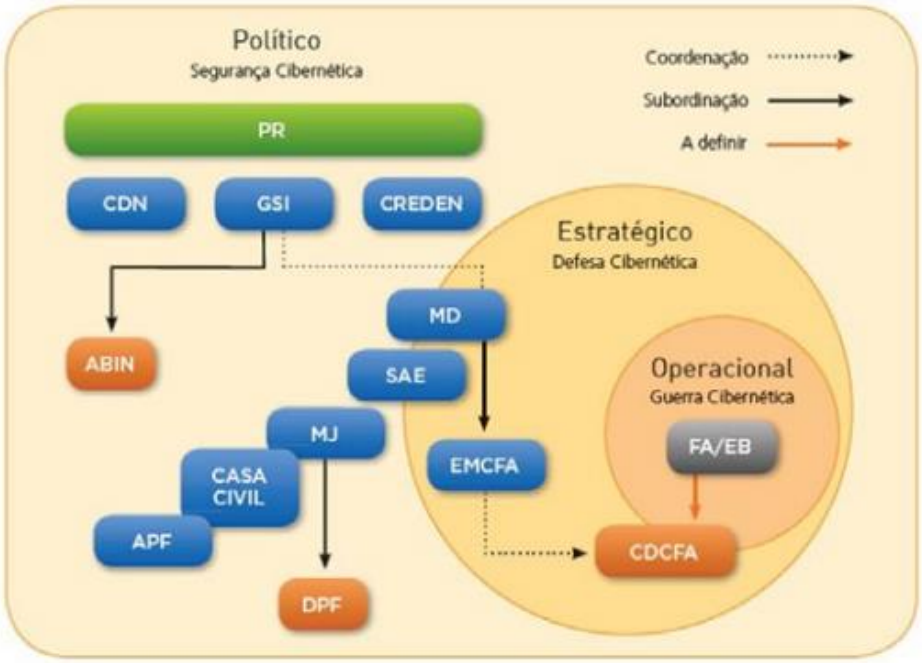
A pirataria de software é o roubo de ativos intelectuais associados a programas de computador, e resulta em perda de lucros para empresas e indivíduos que possuem o software, enquanto recompensa os criminosos que não fizeram o trabalho ou arriscaram os recursos necessários para desenvolver o software.

1.3 Arquitetura Institucional de Cibersegurança do Brasil

Existem inúmeras entidades públicas envolvidas na gestão da segurança cibernética no Brasil. Muitos deles estão focados exclusivamente na gestão de sistemas, desenvolvimento técnico e ferramentas de atualização. Exemplos incluem o CSIRT brasileiro (CERT.br), o Network Information Center (NIC.br, responsável pela gestão do nome de domínio de primeiro nível do país), o Centro de Segurança da Informação de Renato Archer, do Ministério da Ciência e Tecnologia, SERPRO, e INI, entre muitos outros. Uma proporção menor está preocupada com o campo da segurança cibernética como um todo. Dependendo da agência, pode estar envolvida na elaboração de diretrizes normativas, na adoção de decisões políticas ou na autorização de ações em nível nacional e local (DINIZ et al., 2014).

A Figura 1 a seguir resume os principais atores que operam no nível federal e que estão envolvidos na formação da arquitetura de cibersegurança do Brasil.

Figura 1. Arquitetura cibernética do Brasil[4]: níveis político, estratégico e operacional



Fonte: Diniz et al., 2014, p. 19

Existe uma hierarquia de instituições estatais envolvidas na gestão da cibersegurança brasileira. No topo da pirâmide está o Gabinete Presidencial de Segurança Institucional (GSI). Em contato direto com o presidente, o GSI é um órgão governamental importante encarregado de lidar com todos os aspectos civis da segurança cibernética. Também é responsável por outras áreas, incluindo assuntos militares e ciberdefesa (faz parte do Conselho de Defesa Nacional, ou CDN) (DINIZ et al., 2014).

Os ramos subordinados do GSI incluem o Departamento de Segurança da Informação e Comunicação (DSIC), responsável por garantir a disponibilidade, integridade, confidencialidade e autenticidade da informação e comunicação para a administração pública federal. Isso é coordenado em estreita consulta com a Casa

[4] Acrônimos da Figura 1: PR: Presidência da República; CDN: Conselho de Defesa Nacional (Conselho de Defesa Nacional); GSI: Gabinete de Segurança Institucional (Gabinete Presidencial de Segurança Institucional); CREDEN: Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo (Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo); ABIN: Agência Brasileira de Inteligência; MD: Ministério da Defesa (Ministério da Defesa); SAE: Secretaria de Assuntos Estratégicos (Secretaria de Assuntos Estratégicos); MJ: Ministério da Justiça (Ministério da Justiça); APF: Administração Pública Federal (Administração Pública Federal)
DPF: Departamento de Polícia Federal (Polícia Federal); EMCFA: Estado-Maior Conjunto das Forças Armadas (Estado-Maior Conjunto das Forças Armadas); CDCFA: Comando de Defesa Cibernética das Forças Armadas (Comando de Defesa Cibernética das Forças Armadas); FA/EB: Forças Armadas / Exército Brasileiro (Forças Armadas / Exército Brasileiro).

Civil (Casa Civil), que também é responsável por supervisionar a concessão de certificados de segurança digital (para infraestruturas públicas essenciais). Também no GSI estão a Secretaria de Assuntos Estratégicos (SAE) e a Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo (CREDEN), uma comissão assessora do Presidente. O trio DSIC, SAE e CREDEN são atores-chave na formação dos debates sobre segurança cibernética no Brasil (DINIZ et al., 2014).

Outras instituições que influenciam a agenda da cibersegurança no Brasil incluem o Departamento de Polícia Federal (DPF), sob a supervisão do Ministério da Justiça (MJ). Embora sua função principal seja a aplicação da lei em nível federal, ela também possui unidades dedicadas à segurança cibernética. Da mesma forma, a Agência Brasileira de Inteligência (ABIN), além de atuar no monitoramento de redes sociais, desenvolveu competências criptográficas para proteção de instituições públicas. Isso é realizado por meio do Centro de Pesquisa e Desenvolvimento em Segurança das Comunicações (CEPESC). Por fim, existe o Ministério da Defesa (MD), que supervisiona as forças armadas e atua como elo de ligação entre civis e militares. Sob o MD está também o Estado-Maior Conjunto das Forças Armadas (EMCFA), que também desempenha um papel na coordenação da resposta cibernética (DINIZ et al., 2014).

2 ABORDAGEM JURÍDICA SOBRE OS CRIMES VIRTUAIS

No século 21, a Internet entrou em uma nova fase em sua existência. Com o surgimento dos crimes cibernéticos, o estabelecimento de políticas para proteger a sociedade contra o crime no ciberespaço se tornou indispensável, enfatizando a necessidade de legislações de acordo com o atual desenvolvimento tecnológico.

A maneira como os países desejam elaborar essas políticas, no entanto, varia de estado para estado, tornando-se uma fonte de conflito no regime de cibercrime. Embora existam muitos regulamentos internacionais a esse respeito, como os da Assembleia Geral, o ECOSOC e os documentos de resultado da WSIS, muitos países parecem estar mais preocupados em abordá-lo em uma base regional, desafiando os compromissos multilaterais e internacionais. É o caso dos regulamentos da União Europeia, da Organização para os Estados Americanos, da Cooperação Econômica Ásia-Pacífico, da Organização de Cooperação de Xangai e da Comunidade Econômica dos Estados da África Ocidental (BORTOT, 2017).

Em 23 de novembro de 2001, ocorreu a Convenção de Budapeste do Conselho Europeu (MAZONI 2009). O tratado elaborado durante a Convenção foi o primeiro tratado internacional a tratar de crimes informáticos, referindo-se especificamente à segurança de redes de computadores, violações de direitos autorais, fraude informática e pornografia infantil. Estados não membros do Conselho da Europa também participaram da Convenção. A Convenção sobre Cibercrime listou algumas medidas a serem tomadas em nível nacional em relação a quatro tipos de crimes cibernéticos (Comitê da Convenção sobre Cibercrime, 2001):

1. Ofensas à confidencialidade, integridade e disponibilidade de dados e sistemas de computadores: como acesso e interceptação ilegal e interferência de dados;

2. Infracções relacionadas com o computador: incluindo falsificação e fraude;

3. Infrações relacionadas ao conteúdo: relacionadas à pornografia infantil; e

4. Ofensas relacionadas a violações de direitos autorais e direitos relacionados.

Esta Convenção visava criar disposições legais para tipos específicos de crimes, bem como promover a cooperação internacional, dada a universalização dos delitos. Além disso, a Convenção destacou a importância de todas as disposições legais estabelecidas pelos Estados Membros para cumprir o respeito dos direitos humanos fundamentais e das liberdades civis, como o direito à privacidade, intimidade, liberdade de expressão e acesso público ao conhecimento e à Internet (FERREIRA et al., 2013).

A Convenção sobre Cibercriminalidade de Budapeste entrou em vigor em 2004 e, dois anos depois, foi lançado o Protocolo Adicional à Convenção sobre Cibercriminalidade, abordando a criminalização de atos de natureza racista e xenofóbica cometidos através de sistemas de computador (MAZONI, 2009). Como o primeiro tratado relacionado ao crime de computador, a Convenção de Budapeste mostrou a extrema importância do assunto e apresentou os meios para tornar o ciberespaço um lugar mais seguro. A Convenção abriu o caminho para novas iniciativas multilaterais e multissetoriais nos níveis global e regional. Além da Convenção de Budapeste, muitas outras medidas regionais, globais e multilaterais foram tomadas para combater o cibercrime (KUNRATH, 2017).

A Organização dos Estados Americanos (OEA) criou o Programa Interamericano Portal de Cooperação em Cibercrime. O Portal visou fortalecer a

cooperação em investigação e repressão de tais crimes, promovendo o intercâmbio de informações e experiências entre seus membros e aconselhando os Estados membros da OEA a melhorar e fortalecer a cooperação com organizações e mecanismos internacionais (Organização dos Estados Americanos, 2011).

A Cooperação Econômica Ásia-Pacífico (APEC), relativa à integridade e segurança do ambiente de comércio eletrônico, também fez grandes avanços em suas discussões ao projetar a “Estratégia para garantir um ambiente on-line confiável, seguro e sustentável” (APEC, 2005). Outras organizações, como a Organização de Cooperação de Xangai (SCO), tiveram discussões mais aprofundadas sobre o assunto. Em 1997, o Grupo dos Oito (G8) lançou um Comunicado de Ministros que incluiu um plano de ação e princípios para combater o cibercrime e proteger dados e sistemas contra comprometimento não autorizado (CHANG, et al., 2003).

As Nações Unidas, especialmente através da Assembleia Geral (AGNU) e do Conselho Econômico e Social (ECOSOC), divulgaram uma série de resoluções relacionadas a esse assunto. Em 2001, a AGNU aprovou uma resolução (A / RES / 55/63) que trata do cibercrime, chamada “Combate ao uso indevido criminal de tecnologias da informação”. Esta resolução enfatizou o papel que os países devem desempenhar internamente na eliminação de refúgios seguros para aqueles que abusam criminalmente das tecnologias da informação (KUNRATH, 2017).

Além disso, observou como essas questões transnacionais devem ser investigadas e processadas por todos os Estados envolvidos de maneira coordenada. Desde então, os países aumentaram a conscientização sobre a importância da educação do usuário para prevenir e combater o uso indevido criminal de TI. Por fim, a resolução também alarmou que as soluções para combater o cibercrime devem levar em conta tanto a “proteção das liberdades e privacidade individuais quanto a preservação da capacidade do governo de combater tal uso indevido criminal” (UNGA, 2001).

No Brasil, em 2012, duas leis contra o cibercrime entraram em vigor: a “Lei Azeredo” e a “Lei Carolina Dieckmann” foram assinadas em leis federais, alterando e revisando a legislação brasileira. Código Penal. O primeiro, define crimes cometidos no ambiente digital e via acesso a dispositivos de tecnologia da informação; o último define a contrafação de cartões de débito e crédito como crime (FERREIRA et al., 2013). As leis sem precedentes abriram as portas para a aprovação da Lei de

Direitos Civis da Internet no Brasil, em 2014. A lei é apontada como uma referência global para legislação internacional que trata da rede global de computadores (MARTINS 2014). Para manter a natureza aberta da rede e com base nos princípios de garantia de neutralidade da rede, liberdade de expressão e privacidade dos usuários (CONGRESSO NACIONAL, 2014), a lei garante os direitos dos usuários, em vez de simplesmente criminalizar os atores.

Esperava-se que o Congresso Nacional aprovasse o Marco Civil já em 2012, mas as controvérsias associadas a duas questões importantes resultaram na desaceleração do processo. A primeira dessas controvérsias estava relacionada à questão da neutralidade da rede. As empresas de telecomunicações tentaram obstruir e atenuar o princípio da neutralidade da rede, buscando limitar as proteções legais. A segunda área polêmica do projeto de lei estava relacionada às violações de direitos autorais. Indústrias que dependem de direitos autorais sendo mantidos exigiram o poder de exigir que os ISPs removam conteúdo ilegal sem um mandado. E, apesar da oposição das indústrias de telecomunicações e direitos autorais, o Congresso agiu para preservar a neutralidade da rede e impedir a remoção arbitrária de conteúdo (exceto em casos de pornografia de vingança).

Embora a intenção original do Marco Civil fosse estabelecer garantias e salvaguardas constitucionais relativas à gestão do ciberespaço brasileiro, também se tornou um ímpeto para uma legislação agressiva de prevenção de crimes cibernéticos. De fato, as primeiras leis de crimes cibernéticos no Brasil foram aprovadas devido a indignação popular sobre um caso de *hacking* amplamente divulgado, que envolveu o vazamento de fotos privadas do e-mail de uma famosa estrela de novela. Um clamor da mídia tradicional e social alimentou a ansiedade crescente sobre a questão ainda não definida da privacidade digital. O Congresso realizou uma sessão de emergência e aprovou um projeto de lei elaborado em 2011 (e outro que vinha definhando desde 1999). O primeiro projeto - que se tornou a lei 12.373/12 - tem implicações significativas para os cibercomuns do Brasil. Um segundo projeto de lei - agora a lei 12.735/12 - foi tão fortemente alterado que sua provável eficácia é questionável. Embora alguns críticos afirmem que a legislação é confusa e incoerente, as leis definem e elaboram com sucesso controles e punições relacionados à atividade na Internet. Por exemplo, atualmente é ilegal “invadir dispositivos de TI”, “obter dados privados” ou “interferir ou interromper os serviços de TI”.

É importante notar que essas estruturas e leis foram aprovadas em um momento em que as autoridades brasileiras começaram a repensar a legislação de justiça criminal, que remonta a 1940. Há mais 40 projetos de lei relacionados ao combate ao crime cibernético aguardando aprovação no Congresso. O acúmulo de pedidos reflete um problema amplamente conhecido relacionado ao legalismo excessivo no sistema político brasileiro; também destaca como o governo brasileiro ainda está mal equipado para responder ao cenário dinâmico e em rápida mudança do crime cibernético.

CONCLUSÃO

No estudo se questionou se a estrutura e mecanismos de prevenção adotados aos crimes virtuais no Direito Penal Brasileiro são suficientes para o enfretamento destes crimes no país.

Diariamente cresce o número de pessoas *online*. A Internet é uma ferramenta de comunicação poderosa, necessitando de intervenção estatal, no sentido de coibir práticas que possam ultrapassar o limite da esfera da liberdade alheia. Nesse sentido, é precípuo que tais condutas sejam tipificadas, para que assim o Estado possa exercer sua função, o que, infelizmente, não ocorre.

Os crimes virtuais geralmente tem uma dimensão internacional. Os e-mails com conteúdo ilegal costumam passar por vários países durante a transferência do remetente para o destinatário, ou o conteúdo ilegal é armazenado fora do país. Nas investigações de crimes cibernéticos, é necessária uma estreita cooperação entre os países envolvidos. Os acordos de assistência jurídica mútua existentes são baseados em procedimentos formais, complexos e muitas vezes demorados e, além disso, muitas vezes não cobrem investigações específicas por computador. Estabelecimento de procedimentos para uma resposta rápida a incidentes, bem como pedidos de cooperação internacional é, portanto, vital.

A segurança cibernética desempenha um papel importante no desenvolvimento contínuo da tecnologia da informação, bem como dos serviços de Internet. O aprimoramento da cibersegurança e a proteção de infraestruturas críticas de informações são essenciais para a segurança e o bem-estar econômico de cada nação. Tornar a Internet mais segura (e proteger os usuários da Internet) tornou-se

parte integrante do desenvolvimento de novos serviços e das políticas governamentais.

As atividades de crimes cibernéticos aumentarão e não serão interrompidas. Portanto, uma abordagem melhor para interromper esse crime cibernético é criar um sistema poderoso que possa parar esse tipo de crime. Além disso, a proteção dos dados do cliente deve ter maior prioridade e colocá-los confidencialmente com alta privacidade.

Nesse sentido, o Brasil avançou, ao elaborar as Leis 12.735/2012 e 12.737/201, mas ainda são insuficientes, visto alterarem dispositivos que não previam, quando foram elaboradas, tipificação das condutas (Código Penal de 1940). O Marco Civil da Internet (Lei 12.964/2014) tornou-se aliado importante no combate aos crimes digitais, mesmo com o cunho civil desta Lei, contribuindo para a investigação dos crimes virtuais.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSEMBLÉIA GERAL DAS NAÇÕES UNIDAS (AGNU). **Combate ao uso indevido criminal de tecnologias da informação**. Resolução da UNGA. Nova York: Nações Unidas, 21 de janeiro de 2001.

BARRETO, Alesandro Gonçalves; KUFA, Karina; SILVA, Marcelo Mesquita. **Cibercrimes e Seus Reflexos no Direito Brasileiro,** Editora Jus Podivm, 2020. Disponível em: <https://www.editorajuspodivm.com.br/cdn/arquivos/1b4e25e378a5ac48e98b3d3861692d94.pdf>. Acesso em 21 Abr 2020.

BORTOT, Jéssica Fagundes. Crimes Cibernéticos: Aspectos Legislativos e Implicações na Persecução Penal com Base nas Legislações Brasileira e Internacional. **VirtuaJus**, Belo Horizonte, v. 2, n. 2, p.338-362, 1º sem. 2017. ISSN - 1678-3425

BRASIL. Congresso Nacional (Brasil). Projeto de Lei: Marco Civil.

CHANG, Weiping, WINGYAN Chung, HSINCHUN Chen e SHIHCHIEH Chau. **Uma perspectiva internacional sobre o combate ao cibercrime**. Berlim: Springer Berlin Heidelberg, 2003.

DINIZ, Gustavo et al. Desconstruindo a segurança cibernética no Brasil: ameaças e respostas. **Igarapé Publicações.** Paper estratégico n. 11, Dezembro, 2014. Disponível em: <https://igarape.org.br/wp-content/uploads/2014/11/Strategic-Paper-11-Cyber2.pdf> Acesso em 28 Jul 2020.

FERREIRA BARRETO; BRANCHER. Lei da Internet Os atos que definem crimes de cibercrime no Brasil são assinados em lei. 2013. Disponível em: <http://www.bkbg.com.br/direito-de-internet-publicadasleis-que-tipificar-crimes-informaticos/?lang=en>. Acesso em 21 Abr 2020.

FERREIRA, Ivette Senise. A Criminalidade Informática. Direito & Internet – Aspetos Jurídicos Relevantes. Editora Edipro, 2011.

GARCIA, Plínio Silva de; MACADAR, Marie Anne; LUCIANO, Edimara Mezzomo. A influência da injustiça organizacional na motivação para a prática de crimes cibernéticos. **JISTEM J.Inf.Syst. Technol. Manag.**, São Paulo , v. 15, e201815002, 2018

GIL, Antonio Carlos. **Métodos e Técnicas de Pesquisa Social**. São Paulo: Atlas, 2006.

KUNRATH, Josefa Cristina Tomaz Martins **A expansão da criminalidade no cyberespaço**. Feira de Santana : Universidade Estadual de Feira de Santana, 2017.

MARTINS, Helena. **Entenda o Marco Civil da Internet**. 2014. Disponível em: http://www.ebc.com. br/noticias/brasil/2014/04/entenda-o-marco-civil-da-internet. Acesso em 21 Abr 2020.

MAZONI, Ana Carolina. **Crimes na Internet e a Convenção de Budapeste**. Centro Universitário de Brasília, 2009.

NUCCI, Guilherme de Souza. **Manual de Direito Penal**. 11. Ed. Rio de Janeiro: Forense, 2015.

OTOBONI, Gustavo Henrique dos Santos. **Crimes Cibernéticos**: Phishing. 02/12/2019. Disponível em: <https://ambitojuridico.com.br/edicoes/revista-191/crimes-ciberneticos-phishing/>. Acesso em 21 Abr 2020.