Curso de Direito Artigo Original

CRIMES CIBERNÉTICOS: IMPUNIDADES

CYBER CRIMES: IMPUNITIES

Acadêmica Caroline Climaco Marsole[1], Adelaine Curvo[2]

1 Acadêmica do Curso de Direito

2 Professora do Curso de Direito

Resumo

O presente trabalho tem como fundamento realizar uma breve análise didática a respeito dos intitulados “crimes cibernéticos”. Portanto, se faz essencial entender o ambiente em que se insere essa modalidade de prática delituosa, o ambiente virtual. Considerando importante salientar, ainda, que a fim de combater a criminalidade e a impunidade dos delitos praticados no ambiente virtual, surgiu a Lei dos Crimes Cibernéticos, conhecida por “Lei Carolina Dieckmann”, de número 12.735 de 2012. Assim, isto posto, o legislador ao não considerar dadas condutas como sendo, propriamente, crimes cibernéticos, estas passaram a serem conhecidas doutrinariamente como crimes virtuais impróprios. O método usado para a construção desse artigo foi em forma de pesquisa bibliográfica, analisando jurisprudência e legislação, esse tipo de crime cibernético, promove insegurança tanto para a sociedade, quanto para o âmbito jurídico brasileiro. Com isso, é considerado como os principais crimes cibernéticos: Invasão de dispositivos informáticos para disseminação de vírus e malware que coleta dados (e-mail, telefone, dados bancários e etc.), distribuição de material pornográfico e pedofilia, violação de propriedade intelectual (fraudes de identidades), falsificação de dados financeiros, documentos particulares ou cartões de credito, extorsão cibernética (quando o criminoso exige dinheiro para impedir o ataque á vitima), ataques de ransomware, que bloqueia o acesso ao sistema infectado e cobra resgate em criptomoedas, cryptojacking (invasão de computadores para mineração de criptomoedas, interrupção ou perturbação em sites ou perfis para disseminar mensagens com critério ameaçadoras, e por fim, golpes ou fraudes por meios de redes sociais, anúncios falsos, entre outros.

Palavras-Chave: Crimes Cibernéticos. Lei “Carolina Dieckmann”. Crimes virtuais.

ABSTRACT

The present work is based on a brief didactic analysis regarding the so-called “cyber crimes”. Therefore, it is essential to understand the environment in which this type of criminal practice is inserted, the virtual environment. Considering that it is also important to point out that in order to combat crime and impunity for crimes committed in the virtual environment, the Cyber Crimes Law, known as the “Carolina Dieckmann Law”, number 12,735 of 2012 was created. legislator by not considering certain conducts as being, properly speaking, cyber crimes, these have come to be known doctrinally as “inappropriate virtual crimes. The method used for the construction of this article was in the form of a bibliographical research, analyzing jurisprudence and legislation, this type of cyber crime, promotes insecurity both for society and for the Brazilian legal framework. With this, it is considered as the main cyber crimes: Invasion of computer devices to spread viruses and malware that collects data (e-mail, telephone, bank details, etc.), distribution of pornographic material and pedophilia, violation of intellectual property (identity fraud), falsification of financial data, private documents or credit cards, cyber extortion (when the criminal demands money to prevent the victim from attacking), ransomware attacks, which block access to the infected system and

charge a ransom in cryptocurrencies, cryptojacking (invasion of computers to mine cryptocurrencies, interruption or disruption of websites or profiles to disseminate messages with threatening criteria, and finally, scams or fraud through social media, false advertisements, among others.

Keywords: Cybercrimes. "Carolina Dieckmann" Law. Virtual crimes.

Contato: caroline.marsole@sounidesc.com.br, adelaine.curvo@unidesc.edu.br

1. INTRODUÇÃO

O presente artigo, tem como objetivo principal expor e informar o funcionamento da prática dos crimes cibernéticos, bem como, busca assegurar uma proteção maior aos usuários das redes, para que futuramente essas práticas diminuam e os infratores sejam devidamente punidos.

Crime Cibernético como o nome sugere é uma prática criminosa, que faz utiliza-se de uma rede de computadores ou um dispositivo que esteja conectado em rede, tipificado no o art. 154-A do Código Penal como: 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 vantagens ilícita.

O presente trabalho pretende discutir e analisar as questões dos crimes cibernéticos, os efeitos causados e recursos encontrados pelo governo, para prevenir tais práticas criminosas. O primeiro tópico indica um breve histórico do seu surgimento, e de seus avanços.

A internet tornou-se uma das principais ferramentas dos criminosos, pois por meio de informações pessoais, através de dados comerciais, facilita em grande espaço para as práticas ilícitas. Já, no segundo tópico existe uma análise sobre toda a evolução histórica e legislativa, com destaques nas legislações brasileiras. Com total importância na lei de nº 12.737/2012 Lei Carolina Dieckamnn.

Essa legislação catalogou as condutas penais típicas, mas não reconhecendo a existência de várias condutas delitivas aplicadas no mundo. O

terceiro tópico analisa os crimes praticados em esfera virtual mostrando diversos crimes cibernéticos, seus autores e as dificuldades para puni-los. Os principais delitos cibernéticos praticados no Brasil são: pornografia infantil; fraudes bancarias; crimes contra honra, a apologia e incitação aos crimes contra vida e o tráfico de drogas. CPF, computadores e dispositivos conectados à Internet também são diferenciados na forma, através do endereço IP. Este número de protocolo é único e permite a comunicação na rede, portanto, o endereço IP é um dos pontos de identificação do agente do crime.

Logo, as dificuldades começam na tentativa de obter este IP, pois embora eles possam ser descobertos a partir dos gerenciadores de sites de acesso à Internet ou, obtendo o do usuário que estava acessando naquele momento é complexo burocrático.

Atualmente a utilização da internet vem tomando conta do cotidiano e da rotina das pessoas. Pela facilidade de acesso, pessoas de todo mundo se conectam em busca de relações profissionais, pessoais de cunho envolvendo relações (amorosas, amizades) e até mesmo pessoas com más intenções e objetivo de aplicar golpes.

Para efeito deste estudo, adotaremos o conceito de crime cibernético, por entender-se como termo suficientemente abrangente, abarcando diversas condutas delitivas que se utilizam ou que se voltam contra dispositivos e recursos computacionais. De maneira objetiva, pode-se conceituar crimes cibernéticos como sendo condutas ilegais que se efetivam mediante a utilização de dispositivos informáticos, conectados ou não a rede mundial de computadores, bem como as ações criminosas contra equipamentos tecnológicos, sistemas de informação ou banco de dados.

A metodologia aplicada foi a revisão de literatura, partindo da situação problema que originou o estudo, qual seja: como criar medidas preventivas para prevenir a população? O objetivo foi coletar dados a fim de contribuir ainda que de forma científica para a formação de futuras políticas de prevenção ao tipo de crime tecnológico.

2. CONTEXTO HISTÓRICO

2.1 EVOLUÇÃO HISTÓRICA DA INTERNET

Em ordem cronológica, o surgimento da internet precedeu o surgimento da Web. O conceito remonta ao início dos anos 1960 como um projeto da empresa de Pesquisa e Desenvolvimento (RAND) financiada pela robustez aérea dos estados unidos da américa para o desenvolvimento de redes de comunicações militares que arrostam a ataques nucleares.

A preocupação de que as autoridades de defesa do governo norte-americano tenham redes de comunicações seguras no pior cenário decorreu do período histórico vivido pelo país conhecido mundialmente como Guerra Frígida.

Anos depois, em setembro de 1969, ainda sob pressão da disputa velada com a antiga associação das Repúblicas Socialistas soviéticos (URSS), o departamento de Defesa dos Estados Unidos, por meio de sua agência de pesquisa, a Project Agency Advanced (ARPA), lançou a ARPANET. A rede de computadores que deu origem ao que hoje é chamado de Internet (CASTELLS, 2015).

Segundo Capron e Johnson (2004), primeiras conexões estabelecidas pela ARPANET, em 1969, foram entre as seguintes instituições acadêmicas: Universidade da Califórnia em Los Angeles (UCLA); instituto de Pesquisa de Stanford (SRI); Universidade da Califórnia Introdução à seção 12 U1 - Estória e Evolução da internet em santa Bárbara (UCSB); Universidade de Utah. Na Ilustração 1.1, fica evidente a importância da ARPANET, pois inicialmente conectava apenas as quatro instituições de ensino mencionadas, que já estavam fisicamente distantes, em 1977 sua infraestrutura de rede cruzava os extremos dos Estados Unidos.

A partir de 1988, quando a rede mundial de computadores passou a ser implementada no Brasil, a época não houve preparos e investimentos para combater os crimes que já vinham sendo praticados nos países que originaram a internet, de modo que ficou mais fácil a prática de crimes na rede no território brasileiro. (CRUZ; RODRIGUES, 2018).

2.2 NORMAS REGULAMENTADORAS

O vazamento das fotos íntimas da atriz Carolina Dieckmann, em maio de 2012, foi capaz de agilizar as negociações e tratativas acerca da matéria,

promovendo a promulgação da Lei n. 12.737/12, que veio a ser chamada de “Lei Carolina Dieckmann”.

Outro problema encontrado para as investigações serem mais precisas é que no nosso ordenamento jurídico a sanção penal só pode ser aplicada, quando houver a certeza da prática do crime, sendo fundamentais a comprovação da autoria e da materialidade, ou a existência de fortes indícios de que o sujeito praticou o crime. Caso não consiga ser comprovada a materialidade e autoria, o juiz poderá absolver o réu, conforme traz o artigo 386 do Código de Processo Penal (CPP) (CRUZ E RODRIGUES, 2018).

> Art. 386. O juiz absolverá o réu, mencionando a causa na parte dispositiva, desde que reconheça: I - Estar provada a inexistência do fato; II - Não haver prova da existência do fato;
>
> III - Não constituir o fato infração penal;IV - Estar provado que
>
> o réu não concorreu para a infração (...) V - Não existir prova
>
> de ter o réu concorrido para a infração penal;

De modo geral, é possível verificar uma tendência da doutrina em adotar um entendimento mais amplo, abrangendo não apenas dados, mas também os computadores, sistemas em rede e demais dispositivos informáticos. Segundo WANG (2016 p. 251), esta posição possui fundamentação na inexistência de uma correlação estrita entre os componentes digitais e materiais, visto que a afronta às informações digitais não necessariamente resultaria em danos ao aparelho que as armazena (e vice-versa).

No entanto, ainda que ordenamento jurídico brasileiro já possua algumas leis que versam sobre a temática da criminalidade cibernética, é preciso destacar a incipiência de tal produção legal, haja vista que, além de diminuta, apresenta-se repleta de lacunas e ambiguidades, dificultando o enfrentamento prático desses delitos (MINSKI, 2018, p. 24).

2.3 O SER HUMANO E A NECESSIDADE COTIDIANA DA INTERNET

Atualmente o uso da internet é algo habitual e cotidiano para as pessoas. Com a facilidade de informações e processos, pessoas de todo mundo se conectam em busca de facilidade e agilidade. Exemplo disso são os aplicativos de relacionamentos, operações bancárias através de aplicativos, entre outros.

No entanto, com as novas tecnologias despontaram também novos riscos, muitos dos quais até então inimagináveis – dentre eles, os crimes cometidos no âmbito da informática. (MINSKI, 2018, p. 9)

Através deste ponto, nota-se grande problema relacionado ao Estado brasileiro em punir os agentes que praticam o cibercrime. As pessoas relacionam a "impunidade" com a inexistência de leis próprias para os crimes cibernéticos. A grande dificuldade encontrada para punir os criminosos das práticas na internet conforme já foi mencionada não ocorre pela falta de norma que caracteriza os crimes e os classifica em uma ordem. O real problema se presencia em detalhes como a falta de tecnologia e de mão de obra especializada para o combate aos cibercrimes.

2.4 TIPICIDADE PENAL DOS CRIMES CIBERNÉTICOS FRENTE A LEGISLAÇÃO BRASILEIRA

O artigo 1º do Código Penal Brasileiro diz: "Não há crime sem lei anterior que o defina. Não há punição sem prévia sanção legal". Cujo crime é a violação de normas estabelecidas por lei e que, se não houver normas, não se pode falar em crime. Ao contrário da crença popular, os crimes cometidos na Internet têm tipificação e quando os infratores são identificados, há uma sanção criminal. O fato de não ter o termo "internet" no preâmbulo, leva as pessoas a crerem que sempre há impunidade nos crimes cibernéticos. Vejamos:

QUADRO 1

CRIME	**TIPIFICAÇÃO**	**FUNDAMENTAÇÃO**
Assédio Sexual	Constranger alguém com o intuito de obter vantagem ou favorecimento sexual, prevalecendo-se o agente da sua condição de superior hierárquico ou ascendência inerentes ao exercício de emprego, cargo ou	216-A do Código Penal Brasileiro

	função. Pena detenção, de 1 (um) a 2 (dois) anos.	
Discriminação	**Art. 20**. Praticar, induzir ou incitar, pelos meios de comunicação social ou por publicação de qualquer natureza, a discriminação ou preconceito de raça, por religião, etnia ou procedência nacional. c/c **Art. 140**. Injuriar alguém, ofendendo-lhe a dignidade ou o decoro. (...) § 3º Se a injúria consiste na utilização de elementos referentes a raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência	Regulamentada pela Lei nº 7.716/89 de 1989, combinado (c/c) com o artigo 140 do Código Penal Brasileiro, que trata dos crimes de raça ou de cor, em seu art. 20
Calúnia; Difamação; Injúria.	**Art. 138** – Caluniar alguém, imputando-lhe falsamente fato definido como crime; (...) **Art. 139** – Difamar alguém, imputando-lhe fato ofensivo à sua reputação: (...) **Art. 140** – Injuriar alguém, ofendendo-lhe a dignidade ou o decoro: (...).	Tipificados nos artigos 138, 139 e 140 do Código Penal Brasileiro
Apologia ao Crime	Fazer, publicamente, apologia de fato criminoso ou de autor de crime: Pena – detenção, de três a seis meses, ou multa.	Tipificação legal no artigo 287 do Código Penal Brasileiro

Pornografia Infantil	Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente; Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.	Estabelecido no artigo 214-A do Código Penal Brasileiro
Estelionato	Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: Pena – reclusão, de um a cinco anos, e multa.	Artigo 171 do Código Penal Brasileiro
Roubo de identidade	Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem: Pena - detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave. Pena - detenção, de três meses a um ano, ou multa, se o fato não	Regulamentado no Artigo 307 do Código Penal

	constitui elemento de crime mais grave.	

De acordo com ROCHA (2020, p.163) embora o preâmbulo não mencione "internet", o fato de sujeitos que utilizam a rede como meio de cometer os ilícitos, o consumo tem uma tipificação para que as penalidades possam ser aplicadas. Portanto, aqui estão os crimes mais comuns praticados pela internet, com as devidas providências.

Esses crimes necessitam da intervenção do Estado, mas, não se limitam a, ações judiciais por violação de direitos autorais, ações judiciais por difamação, ações judiciais por uso ilegal de informações confidenciais, processos criminais por fraude eletrônica e ações judiciais por assédio na Internet. Além disso, a Pessoa Segura pode enfrentar restrições às suas atividades na Internet, tais como a limitação do acesso a determinados sites ou a remoção de conteúdo ilegal de sites de redes sociais.

Conforme TEIXEIRA (2013, p.49), segundo o pensamento de Wendt, traz o rol de delitos praticados no Brasil que são mais comuns atualmente. Neste mesmo rol, destaca-se as fraudes bancárias, os crimes contra honra como a calúnia, a difamação e injúria.

O Marco Civil da Internet trouxe grande regulamentação sobre como os dados na internet devem ser administrados, porém, a nível de combate a crimes, mas ainda existe ausência de legislação bem elaborada e específica, algo fundamental para o amparo dos usuários acometidos pelas condutas atípicas que não podem ser punidas em decorrência do princípio da reserva legal (BORTOT, 2017). No entanto, vejamos agora os crimes previstos no Código Penal Brasileiro nesse âmbito online:

QUADRO 2

CRIME	**TIPIFICAÇÃO**	**FUNDAMENTAÇÃO**
Pornografia infantil online	Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo	Art. 241 do ECA (Estatuto da Criança e do Adolescente)

	explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.	
Fraude Bancária Eletrônica	§ 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo. (Incluído pela Lei nº 14.155, de 2021) § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional. (Incluído pela Lei nº 14.155, de 2021). § 3º - A pena aumenta-se de um terço, se o crime é cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência.	A Lei nº 14.155, de 2021 alterou o Código Penal, criando a figura da Fraude Eletrônica, estando prevista nos § 2º-A, § 2º-B e § 3º do artigo 171.

Violação a direitos autorais	Violar direitos de autor e os que lhe são conexos: Pena – detenção, de 3 (três) meses a 1 (um) ano, ou multa.	Art. 184 do Código Penal Brasileiro
Divulgação indevida de dados sigilosos	Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem.	Tipificação legal no artigo 153 do Código Penal Brasileiro
Atribuição de falsa identidade	Art. 307. Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem Art. 308. Usar, como próprio, passaporte, título de eleitor, caderneta de reservista ou qualquer documento de identidade alheia ou ceder a outrem, para que dele se utilize, documento dessa natureza, próprio ou de terceiro	Estabelecido no artigo 307 e 308 do Código Penal Brasileiro
Estelionato eletrônico	Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro	Artigo 171 do Código Penal Brasileiro

	meio fraudulento: Pena – reclusão, de um a cinco anos, e multa.	
Violação da imagem e da honra	Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação. Art. 141, III - na presença de várias pessoas, ou por meio que facilite a divulgação da calúnia, da difamação ou da injúria.	Regulamentado no Artigo 139 e 141, III do Código Penal Brasileiro
Interceptação clandestina de dados	Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.	Presente no Art. 10 da lei 9296/96
Alteração indevida de sistemas de informação do Governo	Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano	Art. 313-A do Código Penal Brasileiro, incluído pela Lei nº 9.983, de 2000

Contudo, a polícia tem o dever de investigar e punir as condutas ilícitas praticadas no mundo virtual. A era da informática facilita o fenômeno conhecido

como globalização, além de facilitar a informação, ela gerou novas formas de práticas ilícitas surgindo assim os crimes cibernéticos. (FOGLIATTO, 2019).

3. CONTRIBUIÇÕES BIBLIOGRÁFICAS

De acordo com os pesquisadores MATSUYAMA e LIMA (2017) faz-se necessário esclarecer que, doutrinariamente, não há consenso sobre a terminologia adequada para se conceituar crime cibernético, vislumbrando-se o emprego de diversos termos para caracterizá-lo como: crimes digitais, crimes eletrônicos, crimes informáticos, e-crimes, crimes virtuais, dentre outros. Nessa perspectiva, assevera Patrícia Santos da Silva:

> [...]que não há uma nomenclatura sedimentada pelos doutrinadores acerca do conceito de crime cibernético. De uma forma ou de outra o que muda é só o nome atribuído a esses crimes, posto que devem ser observados o uso de dispositivos informáticos, a rede de transmissão de dados para delinquir, o bem jurídico lesado, e ainda deve a conduta ser típica, antijurídica e culpável. (DA SILVA, 2015, p.39).

Para efeito deste estudo, adotaremos o conceito de crime cibernético, por entender-se como termo suficientemente abrangente, abarcando diversas condutas delitivas que se utilizam ou que se voltam contra dispositivos e recursos computacionais. De maneira objetiva, pode-se conceituar crimes cibernéticos como sendo condutas ilegais que se efetivam mediante a utilização de dispositivos informáticos, conectados ou não a rede mundial de computadores, bem como as ações criminosas contra equipamentos tecnológicos, sistemas de informação ou banco de dados. Nesse sentido assevera Aldemario Araujo Castro:

> [...] são denominados de "crimes de informática" as condutas descritas em tipos penais realizadas através de computadores ou voltadas contra computadores, sistemas de informática ou os dados e as informações neles utilizados (armazenados ou processados). (CASTRO, 2003, p.1).

Segundo ORRIGO e FILGUEIRA (2015, p. 5), existem várias classificações doutrinárias sobre a natureza jurídica dos crimes cibernéticos. Mas em seu artigo, os mesmos adotam a vertente que divide os crimes em: crimes cibernéticos próprios e impróprios. Os crimes cibernéticos próprios são aqueles em que o agente, para cometer um delito, necessita do computador, ou seja, o computador é o meio de execução essencial. Os bens jurídicos afetados, pelos crimes cibernéticos próprios

são os dados armazenados em outra máquina ou rede. O delito é cometido por meio do computador e se consuma também pelo meio informático.

Em nossa legislação, um exemplo é a invasão de um dispositivo de computador. O cibercrime impróprio também é cometido por meio do computador, mas o bem jurídico aqui violado pode ser afetado de “n” maneiras, não necessariamente pelo uso do computador, ou seja, a máquina não é essencial, o crime afeta o mundo físico além da tecnologia da informação. Seguem-se exemplos de ofensas irracionais descritas na nossa legislação: calúnia; injúria; difamação; ameaça; furto; apropriação indébita; estelionato; dano; violação ao direito autoral; pedofilia; crime contra a propriedade intelectual. Observe que todos eles podem ser transferidos sem usar o computador, mas também é possível cometê-los usando o computador como meio.

Conforme ALEXANDRE JÚNIOR (2019), O cibercrime nada mais é que todo ato em que o computador ou meios de tecnologia de informação serve para atingir um ato criminoso ou em que o computador ou meios de tecnologia de informação é objeto de um crime. O cibercrime está associado ao fenômeno da criminalidade informacional de condutas violadoras de direitos fundamentais, seja por meio da utilização da informática para a prática do crime ou como elemento de tipo legal de crime.

Em sentido amplo, a criminalidade informática engloba toda atividade criminosa realizada por computadores ou meios de tecnologia da informação. Em sentido stricto, a criminalidade informação engloba crimes, de acordo com Simas (2014, p. 12), “quem que o meio informático surge como parte integradora do tipo legal, ainda que o bem jurídico protegido não seja digital”.

3.1 CRIMES CIBERNÉTICOS NO BRASIL - ORIGEM HISTÓRICA E CONTEMPORÂNEA;

Essa modalidade de delito começou a ganhar destaque no ordenamento jurídico brasileiro a partir da lei 12.737 de 2012, popularmente denominada lei Carolina Dieckmann.

Essa lei foi criada em virtude de a atriz que dá nome à lei ter sido vítima de ataques cibernéticos e, em decorrência, teve fotos íntimas disponibilizadas na rede

sem o seu consentimento. Com efeito, referida lei impôs alterações no Código Penal para tipificar os chamados crimes informáticos, a exemplo da inclusão do artigo 154-A, que tipifica a conduta de quem invade dispositivo alheio com o fim de obter, adulterar ou destruir dados ou informações sem autorização tácita ou expressa do titular do dispositivo. Essa conduta previa pena de detenção de 3 (três) meses a 1 (um) ano, além de multa.

Como se vê, a pena para o delito descrito acima era extremamente branda e muito frágil do ponto de vista técnico.

Com o agravamento da pandemia causada pelo novo coronavírus, foi perceptível um exponencial aumento de delitos causados por meio da internet, razão pela qual ensejou o PL 4.554/2020, que previa a modalidade qualificada dos crimes de furto e estelionato por meio da internet, com o consequente aumento de pena para referidos delitos.

Aludido projeto foi aprovado pelo Congresso Nacional, sendo transformado na lei 14.155/2021 sancionada pelo Presidente da República, com efeitos de aplicabilidade imediata.

Conforme PINHEIRO (2013), trata-se de um importante avanço no combate aos crimes praticados pela internet, na medida em que acrescenta ao Código Penal o agravante do furto qualificado, cuja pena será de 4 (quatro) a 8 (oito) anos de reclusão e multa. Ainda, prevê aumento da pena se praticado em desfavor de idosos ou com uso de servidor mantido fora do país.

A referida lei também traz alterações ao crime de estelionato, incluindo a modalidade qualificada na hipótese de a vítima ser enganada e fornecer informações por meio da internet. Agora a pena que era de 1 (um) a 5 (cinco) anos, passando agora a prever, no §2º-A, a pena de 4 (quatro) a 8 (oito) anos de reclusão. Além de agravar a pena do já citado delito tipificado no artigo 154-A do Código Penal para 1 (um) a 4 (quatro) anos de reclusão, passando a ser de 2 (dois) a 5 (cinco) anos de reclusão, se dá invasão do dispositivo resultar na obtenção de conteúdo privado.

3.2 CONVENÇÃO DE BUDAPESTE SOBRE CIBERCRIME

A Convenção de Budapeste, celebrada na Hungria em 23 de novembro de 2001 pelo Conselho da Europa, teve como signatários 43 países, europeus, em sua

maioria. Cada Estado signatário deve ratificar as disposições constantes da Convenção no seu ordenamento jurídico interno.

A Convenção de Budapeste foi o resultado de um trabalho desenvolvido pelo Conselho da Europa, na qual estava sendo priorizada a proteção da sociedade contra a criminalidade no ciberespaço. Visava a escolha de uma legislação comum que tivesse o objetivo de uma maior cooperação entre os Estados da União Europeia, sendo que tal tarefa já vinha sendo desenvolvida desde a década de 1990.

Com a efetivação da Convenção de Budapeste, adotada em 2002 pelo Conselho da Europa, e a abertura à assinatura por todos os países que a desejarem, ficou demonstrada a atualidade desta nova modalidade de crime e a necessidade de ele ser combatido por toda a sociedade mundial, visto que não só atinge a Europa, mas todo o mundo.

Art. 37 – Adesão a Convenção

1. Após a entrada em vigor da presente Convenção, o Comitê de Ministros do Conselho da Europa pode, depois de ter consultado os Estados contratantes da Convenção e de ter obtido o acordo unânime, convidar qualquer Estado não membro do Conselho e que não tenha participado de sua elaboração, a aderir à presente Convenção. A decisão é tomada pela maioria prevista no art. 20, alínea d, dos Estatutos do Conselho da Europa e por unanimidade dos Estados contratantes com direito de voto no Conselho de Ministros.

2. Em relação a qualquer Estado aderente a Convenção, em conformidade com o nº 1, a Convenção entrará em vigor no primeiro dia do mês seguinte ao termo de um período de três meses após a data do depósito do instrumento de adesão junto ao Secretário Geral do Conselho da Europa.

4. CONSIDERAÇÕES FINAIS

A internet surgiu como um meio de comunicação militar para transmitir segredos, logo depois se popularizou e tornou-se civil com muitos adventos e formas de conectar o mundo. Mas, como toda nova invenção, surgiram também formas de prejudicar o próximo, os chamados crimes cibernéticos. E desde então tem crescido

cada vez mais em e de forma global. Mas com tanta inovação e o grande crescimento desse meio, infelizmente acabou virando uma arma, sendo praticados através dele inúmeros crimes que só aumentam a cada dia. Afinal, usamos o tempo todo e para tudo. Com isso, para aqueles que praticam esses atos criminosos, é necessário realizar as investigações necessárias para que seja aplicada a punição adequada que mais se aplica aos atos. Portanto, é importante que estejamos sempre atentos à jurisdição sobre esses crimes virtuais.

Atualmente a utilização da internet vem se apropriando do cotidiano e da rotina das pessoas. Com facilidade de acesso, pessoas de todo mundo se conectam em busca de relações profissionais e pessoais de cunho pessoal (amorosas, amizades) e até mesmo pessoas com intenções ruins objetivando aplicar golpes.

Com o presente artigo, foi possível analisar especificamente os crimes, com o fim de demonstrar a necessidade de uma regulamentação jurídica própria ao tema, verificando também, a possibilidade de responsabilização dos provedores de Internet para colaboração com a Justiça. Ademais, também visou esclarecer o modo de como se estabelece o poder judiciário nesse sentido e as fases do processo penal tendo em vista que as sanções devem ser aplicadas pela lei.

Com base nisso, os crimes cibernéticos mais cometidos são:

- Plágio;
- Invasão de dispositivos informático/furto de dados;
- Calúnia, difamação e injúria;
- Incitação/ apologia ao crime;
- Pornografia infantil;
- Racismo/ LGBTfobia/ Misoginia;
- Pirataria digital;
- Divulgação de fotos íntimas;
- Criação de perfil fake.

Sendo assim, é possível observar a importância dos cuidados mediante aparelhos eletrônicos e redes sociais. Afinal, são os nossos maiores aliados diante da nossa realidade tecnológica.

5. REFERÊNCIAS

AQUIM, Teixeira. 2017. Proteção de Dados: um Desafio Para os Data Centers. Disponível em: http://www.datacenterdynamics.com.br/focus/archive/2017/04/prote%C3%A7%C3%A3o-de-dados-u m-desafio-para-os-data-centers. Acesso em: 16 de novembro de 2019.

Boletim Jurídico, Uberaba/MG, a. 19, nº 990. Disponível em: *https://www.boletimjuridico.com.br/artigos/direito-penal/10382/crimes-virtuais-conceito-formas-inve stigacao*. Acesso em 20 set. 2022.

BORTOT, Jessica 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, 2017.

CASTRO, Aldemario Araujo. A internet e os tipos penais que reclamam ação criminosa em público. Disponível em: Acesso em 15 de setembro
LIMA, Adriano Gouveia; DUARTE, Adrienne..Crimes virtuais: conceito e formas de investigação.

CÓDIGO PENAL BRASILEIRO. 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848. Acesso em 20 set. 2022.

CRUZ, D.; RODRIGUES, J. Crimes cibernéticos e a falsa sensação de impunidade. Revista Científica Eletrônica do Curso de Direito, v. 13, jan. 2018.

DA SILVA, Patrícia Santos. Direito e crime cibernético: análise da competência em razão do lugar no julgamento de ações penais. Brasília: Vestnik, 20.

FOGLIATTO, Juliana. Os Crimes Cibernéticos e os Meios que a Polícia Utiliza Para a Identificação dos Criminosos. 2019.

JÚNIOR, Júlio César ALEXANDRE. CIBERCRIME: UM ESTUDO ACERCA DO CONCEITO DE CRIMES INFORMÁTICOS. **Revista Eletrônica da Faculdade de Direito de Franca**, v. 14, n. 1, p. 341-351, 2019.

MATSUYAMA, Keniche Guimarães; LIMA, João Ademar de Andrade. **Crimes cibernéticos**: atipicidade dos delitos. 2017.

MINSKI, Bruno Henrique Zanette. CRIMES CIBERNÉTICOS E A RESPONSABILIDADE DOS PROVEDORES: Uma análise conceitual e legislativa sob a ótica da sociedade de informação e do risco. Curitiba, 2018.

ORRIGO, Gabriel Marcos Archanjo; FILGUEIRA, Matheus Henrique Balego. CRIMES CIBERNÉTICOS: UMA ABORDAGEM JURÍDICA SOBRE OS CRIMES REALIZADOS NO ÂMBITO VIRTUAL. v. 11, n. 11 (2015).

PINHEIRO, Patrícia Peck. Direito Digital. 5. Ed. São Paulo: Saraiva, 2013. Disponível em: https://www.migalhas.com.br/depeso/347513/crimes-ciberneticos--avanco-legislativo-no-brasil.