PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
PRO-REITORIA DE GRADUAÇÃO
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
CURSO DE DIREITO
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

CRIMES CIBERNÉTICOS – A PERÍCIA TÉCNICA (LEI CAROLINA DIECKMANN)

ORIENTANDO : FELIPE THIAGO PORFÍRIO DE MENDONÇA
ORIENTADORA : Profa. Ms. Silvia Maria Gonçalves Santos de Lacerda Santana Curvo

GOIÂNIA-GO
2023

FELIPE THIAGO PORFÍRIO DE MENDONÇA

CRIMES CIBERNÉTICOS – A PERÍCIA TÉCNICA

(LEI CAROLINA DIECKMANN)

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação da Pontifícia Universidade Católica de Goiás

Orientadora: ***Profª. Ms. Silvia Maria Gonçalves Santos de Lacerda Santana Curvo***

GOIÂNIA-GO
2023

FELIPE THIAGO PORFÍRIO DE MENDONÇA

CRIMES CIBERNÉTICOS – A PERÍCIA TÉCNICA
(LEI CAROLINA DIECKMANN)

Data da Defesa: ____ de _____ de _____

BANCA EXAMINADORA

_____
Orientadora: Profª: Ms. Silvia Maria Gonçalves Santos de Lacerda Santana Curvo
Nota

_____
Examinador Convidado: Prof.: Me. Eurípedes Clementino Ribeiro Júnior Nota

CRIMES CIBERNÉTICOS – A PERÍCIA TÉCNICA (LEI CAROLINA DIECKMANN)

Felipe Thiago Porfírio De Mendonça
Silvia Maria Gonçalves Santos de Lacerda Santana Curvo

Este artigo tem por objetivo analisar em que medida a perícia forense pode contribuir para desvendar crimes cibernéticos. Nesse contexto, também é necessário examinar as Leis nº 12.737, de 30 de novembro de 2012, Lei Carolina Dieckmann, e as Leis 12.965, de 23 de abril de 2014, popularmente conhecidas como "Marco civil da internet", responsáveis pela padronização de princípios, direitos e deveres de uso da Internet no Brasil, com o objetivo de regular o uso da Internet e prevenir práticas criminosas. Em outras palavras, a aplicação desta lei visa proteger os direitos da pessoa e sua integridade em ambiente virtual. Embora o tema desperte grande interesse, dada sua relevância e dimensão, por precaução, cabe destacar que o ponto principal deste trabalho gira em torno da ineficácia da Lei Carolina Dieckmann. Impossível não pensar que se tratou de um grande avanço legislativo, porém deixou lacunas, necessitando, assim, de estudos mais aprofundados.

Palavras-chave: Crimes virtuais. Perícia. Lei 12.737/12.

ABSTRACT

This article aims to analyze the extent to which forensic expertise can contribute to uncovering cyber crimes. In this context, it is also necessary to examine Laws nº 12,737, of November 30, 2012, Carolina Dieckmann Law, and Laws 12,965, of April 23, 2014, popularly known as "Marco civil da internet", responsible for the standardization of principles , rights and duties to use the Internet in Brazil, with the aim of regulating Internet use and preventing criminal practices. In other words, the application of this law aims to protect the rights of the person and their integrity in a virtual environment. Although the topic arouses great interest, given its relevance and dimension, as a precaution, it should be noted that the main point of this work revolves around the ineffectiveness of the Carolina Dieckmann Law. It is impossible not to think that this was a major legislative advance, but it left gaps, thus requiring further studies.

Keywords: *Virtual Crimes. Expertise. Law 12,737/12.*

INTRODUÇÃO

No Brasil ocorreram importantes inovações legislativas quanto às leis de proteção de dados no ambiente virtual, como prova disso podemos citar a lei 12.737/12 (Lei Carolina Dieckmann) que trata da tipificação dos crimes virtuais, bem como das sanções e regular os procedimentos. Além disso, a Lei 12.965/14 (Lei

Marco Civil da Internet) estabelece princípios, garantias, direitos e obrigações quanto ao uso da Internet.

No entanto, vale lembrar que nem sempre funcionou, por exemplo, a lei 12.737/12 (Lei Carolina Dieckmann) que não tratou desse fato. Portanto, inúmeros crimes virtuais ainda ocorrem diariamente no Brasil e, portanto, há uma tribulação para obtenção de provas para punir os infratores, como estupradores e estelionatários, das delegacias especializadas que investigam esses crimes, e o aumento da incidência desses crimes, e a ineficácia da Lei Carolina Dieckmann, e as deficiências existentes em relação aos crimes virtuais, e da Lei Geral de Proteção de Dados, Lei n. 13.709/18, que foi alterada pela Lei nº.

Atualmente, o uso da internet tem crescido muito rapidamente, com a revolução tecnológica e as mudanças significativas que dominam a cada dia o estilo de vida da população atual. Portanto, a mídia se tornou mundial com a interação instantânea de milhares de pessoas ao redor do mundo.

Toda essa evolução tem favorecido o surgimento de inúmeros crimes virtuais, causando vulnerabilidade para todas as pessoas cada vez mais interligadas nesse ambiente inovador. Sabe-se que este meio tem fornecido pontos positivos e negativos. Além disso, os infratores detêm muito conhecimento na área de TI, e o utilizam para se beneficiar de práticas criminosas, trazendo assim à tona os crimes digitais/virtuais e, nesse contexto, era necessária uma legislação específica para tratar desses casos, que até então não existiam. existir. Ela só foi prevista pela Lei nº 12.737/12, conhecida como lei Carolina Dieckmann.

Em primeiro lugar, começa com o avanço da Internet que deu origem a toda a evolução tecnológica em curso nos nossos dias, que provocou uma grande transformação do mundo e tem sido a ferramenta essencial para a incidência destes crimes; depois o Marco Civil e a incidência da Lei Carolina Dieckmann, citando dois exemplos de tipos de crimes virtuais, e a Deep Web, e outros meios que são usados para fazer isso para ferir vítimas.

Para tanto, é certo que faltam informações e meios de defesa a serem disponibilizados a todos, o que torna cada dia mais difícil a obtenção de mecanismos efetivos para isso, sua efetiva aplicação da legislação aos infratores e a dificuldade de localizar e procurar o imenso espaço virtual; que na maioria das vezes esses crimes ficam impunes e acabam se agravando, e a LGPD entrou em vigor em 2020.

Para tanto, o presente estudo do artigo tem por objetivo geral analisar em que medida a perícia forense pode contribuir para desvendar crimes cibernéticos. Pretende-se ainda definir crimes cibernéticos, apresentando breve evolução histórica; investigar espécies de crimes cibernéticos; relacionar legislações aplicáveis aos crimes cibernéticos no Brasil, incluindo tratados e convenções internacionais (Convenção de Budapeste); analisar a importância da prova técnica para a formação do convencimento do juiz em processos criminais que envolvam crimes cibernéticos.

A metodologia aplicada neste projeto permite classificar a pesquisa como exploratória, com uso de levantamento bibliográfico para a coleta dos dados. A abordagem do problema é qualitativa, e a análise dos dados é crítica de conteúdo.

1 CRIMES CIBERNÉTICOS

1.1 BREVE EVOLUÇÃO HISTÓRICA

A Internet é um importante canal de pesquisa, interação e relacionamentos humanos, uma criação humana que afeta grande parte da população mundial e, como todas as criações humanas, pode ser usada tanto para o bem quanto para o mal. Dada a sua essencialidade, o Direito tem despertado crescente interesse por ele e pelas consequências jurídicas que produz, conhecer a sua evolução é importante para compreender a evolução dos crimes virtuais (PEREIRA; OLIVEIRA, 2019).

Historicamente, o cibercrime tem mais evidências desde a década de 1960, principalmente em casos de manipulação e sabotagem do sistema. Já em 1970 a figura do hacker era conhecida pelos crimes de invasão e roubo de software. Na década de 1980, tais crimes se espalharam com as práticas de invasão de sistemas, pirataria, pedofilia, entre outras, despertando mais preocupações de segurança virtual (PEREIRA; OLIVEIRA, 2019).

O Brasil, assim como outros países, vem buscando formas de tentar frear o crescimento do cibercrime. Os crimes cibernéticos são meios essenciais para garantir a proteção dos indivíduos, que devem ver respeitada a sua confidencialidade e confidencialidade, conforme explicitado no artigo 5º, inciso X da CF/88, Constituição Federal:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito àvida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> X - São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; (BRASIL, 1988)

No ordenamento jurídico brasileiro existem duas leis norteadoras, sancionadas em 2012, que modificam o código penal e estabelecem sanções para esses crimes. A primeira delas é a Lei de Crimes Cibernéticos (Lei 12.737/2012), conhecida como Lei Carolina Dieckmann, que caracteriza atos como invasão de computadores, roubo de senhas, violação de dados de usuários e divulgação de informações privadas (como fotos , mensagens, etc.). E a segunda é a lei 12.735/12 “Lei Azevedo”, que prevê a instalação de delegacias especializadas no combate aos crimes digitais (COSTA, 2021).

1.2 CONCEITO

Em primeiro lugar, os crimes cibernéticos, também denominados cibercrime, são aqueles que decorrem como resultado de qualquer atividade ilícita realizada no domínio da Internet, por meio de dispositivos eletrônicos, por hackers e crackers (ROSSINI, 2020). Neste sentido, podem ser assim conceituados:

> [...] o conceito de delito informático poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade a confidencialidade (ROSSINI, 2020, p. 110).

A maioria dos crimes cibernéticos também existe no mundo real. Acontece que, além de se desenvolverem e inovarem muito rapidamente, devido aos avanços tecnológicos, muitos comportamentos que se espalham na web têm dificuldade em encontrar o agente que os praticou, pois ocorrem livremente, não encontram barreiras e são anônimos (COSTA, 2021). Sobre eles, se versará mais detidamente na seção seguinte.

1.3 ESPÉCIES DE CRIMES CIBERNÉTICOS

As práticas desses crimes são diversas, sejam crimes de peculato, fraude, falsificação de identidade, *bullying* na Internet, ameaças, entre outros. Tais delitos, para serem classificados como crimes cibernéticos, devem incluir o elemento tecnologia como sendo o principal meio de realização do ato lesivo. Para completar, trata-se de conduta culposa e negligente, que utiliza um sistema eletrônico para implementar a reclamação ilícita (ROSSINI, 2020).

2 LEGISLAÇÕES APLICÁVEIS AOS CRIMES CIBERNÉTICOS NO BRASIL

2.1 O MARCO CIVIL DA INTERNET E A LEI CAROLINA DIECKMANN

O marco civil da Internet surgiu com a Lei de 23 de junho de 2014, n. 12.965, que estabelece as disposições para o uso da Internet em todo o território nacional, como garantias, direitos e deveres de todos diante da evolução tecnológica. Em seus artigos 1º e 3º esta lei prediz sobre princípios e garantias, tal como se demonstra:

> Art. 1º Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria. (BRASIL, 2014)
>
> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> I - Garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II - Proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei; IV - Preservação e garantia da neutralidade de rede;
> V - Preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
> VI - Responsabilização dos agentes de acordo com suas atividades, nos termos da lei; VII - preservação da natureza participativa da rede;
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.
> Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte. (BRASIL, 2014)

Sobre isso, Teixeira (2016) dispõe o seguinte:

> Preocupado com a possibilidade de eventualmente haver alguma limitação à liberdade de expressão ou alguma violação da privacidade dos usuários da internet, o Marco Civil expressa que a garantia a esses dois direitos constitucionais é condição para o pleno exercício do direito à acesso à rede mundial de computador. Ou seja, a violação a esses direitos implica em quebra da própria finalidade do advento do Marco Civil enquanto uma lei federal que objetiva tutelar os usuários da internet (TEIXEIRA, 2016, p. 84).

O Marco Civil da Internet teve como objetivo estabelecer limitações ao uso da Internet e obter direitos, garantias e deveres relativos à rede mundial de computadores, em relação ao direito fundamental à privacidade, e estabelecer a proteção da vida pessoal dos usuários. dados e destacando a necessidade de legislação.

O Projeto n. 35/2012, inicialmente criado pelo projeto de lei n. 2.793/2011, no qual foi proposta a modificação do projeto de lei nº. 84/99 (Lei Azevedo), sendo certificada e publicada pela Lei 12.737/12.

Esta foi a primeira lei criada com o objetivo de combater a ocorrência de crimes cibernéticos. A lei recebeu o nome da atriz Carolina Dieckmann, uma figura pública para quem seu computador pessoal era inválido e suas fotos pessoais foram divulgadas. Devido ao *hype* causado por essa situação, a lei tem sido uma importante ferramenta para punir os crimes cibernéticos.

Ao inserir os artigos 154-A e 154-B do código penal, o legislador autorizou a punição de quem, com a intenção de praticar uma conduta criminosa, sem o consentimento da vítima, invadir um dispositivo informático com o intuito de obter , destruir ou alterar qualquer informação pessoal no dispositivo.

Importa sublinhar que, apesar de ser uma legislação muito importante no combate ao cibercrime, dada a dimensão dos desenvolvimentos tecnológicos, a lei ainda está longe de satisfazer todas as necessidades que estes casos acarretam.

É visível que essas ações causam danos irreparáveis às vítimas, e consequências deploráveis, destinadas a atentar contra sua liberdade e privacidade por se sentirem vulneráveis, até mesmo ao sentimento de impunidade. É lamentável que a legislação não consiga intervir de forma estrita nestas infrações, a pena é mínima face à indenização por toda a sua exposição pessoal, perda de dados pessoais, entre muitos outros constrangimentos.

Fica evidente no texto legal que a conduta do acusado constitui elemento de dolo, uma vez que não pode mencionar a responsabilidade do culpado, portanto, é por meio do dolo que se comete o crime, como pretende o agente praticar a conduta.

Além disso, após o fato, a vítima deve promover sua representação, ou seja, por meio de acusação pública condicional. Portanto, o procedimento continuará a determinar a conduta. É extremamente necessário representar a vítima, para que a investigação criminal e o processo penal possam ser iniciados. Com ações como essas será possível inibir práticas como essas, a fim de diminuir a ineficiência da lei de proteção.

2.2 LGPD

A Lei Geral de Proteção de Dados (LGPD) estabelecida no Brasil a partir da edição da Lei nº 13.709, em 2018, tem por objetivo, e suma, dispor sobre o tratamento de dados pessoais, protegendo os direitos fundamentais de privacidade e liberdade, bem como o livre desenvolvimento da pessoa natural (BRASIL, 2018). Na percepção de Santos e Duarte (2022), trata-se de legislação que é fruto sentida de se regulamentar uma tensão social visível entre o direito de privacidade das pessoas e o controle dos dados pessoais.

Entretanto, segundo Kramar (2021), a partir do momento em que a LGPD entrou em vigor, questões relacionadas à proteção de dados pessoais de um modo geral, que já haviam sido suscitadas em momento anterior, quando da aprovação do Marco Civil da Internet no Brasil pela Lei nº 12.965, de 23 de abril de 2014, também foram reacendidas. Diante disto, Stürmer e Dorfman (2021) fazem importantes apontamentos ao destacarem que, considerando a preponderância que o trabalho tem para o convívio em sociedade da pessoa natural, presume-se que uma legislação com o objeto que tem a LGPD também abarque, de alguma forma, aspectos relacionados ao direito penal.

2.3 TRATADOS E CONVENÇÕES INTERNACIONAIS

2.3.1 Convenção de Budapeste

A Convenção de Budapeste é o tratado internacional sobre crimes cibernéticos, assinado no Conselho da Europa, que busca harmonizar o direito penal e o processo penal, a fim de permitir a cooperação para a obtenção de provas digitais. Foi assinado em 23 de novembro de 2001 e aberto à adesão e ratificação de outros países, tendo sido ratificado por cerca de 52 signatários (COSTA, 2021).

Esta Convenção introduziu inovações na forma de cooperação e regulamentação criminal fora da jurisdição nacional, com o objetivo de combater de forma mais eficiente os crimes cibernéticos. Essa Convenção foi assinada por 43 países e é considerada uma referência legislativa global sobre crimes na web (BITENCOURT, 2020).

Em relação ao acesso a dados que estão armazenados fora do território de cada Estado-parte da Convenção, tem-se previsão constante no artigo 32, adiante transcrito:

> Art. 32. Acesso transfronteiriço a dados informáticos armazenados, com consentimento ou quando são acessíveis ao público.
> Uma parte pode, sem autorização de outra Parte: Investigação e prova nos crimes cibernéticos
> a) aceder a dados informáticos armazenados, acessíveis ao público (fonte aberta), seja qual for a localização geográfica desses dados; ou
> b) aceder ou receber, através de um sistema informático situado no seu território, dados informáticos armazenados, situados no território de outra Parte, se obtiver o consentimento legal e voluntário da pessoa legalmente autorizada a divulgar esses dados, através deste sistema informático.

De todo modo, esta importante Convenção visa defender a sociedade internacional por meio da adoção de leis e da promoção da cooperação internacional. A mencionada Convenção abrange fraudes de informática, violação de direitos autorais, pornografia infantil e invasões de computadores, e também prevê uma série de procedimentos entre países (BITENCOURT, 2020).

Nesse sentido, de acordo com Costa (2021), a Convenção de Budapeste sobre Cibercrime se traduz em um marco importante para a cooperação criminal internacional, com vistas a promover medidas para aprimorar os instrumentos de assistência mútua e produção de provas, bem como a implementação de mecanismos de retenção de provas em forma de dados e celeridade nas investigações e processos criminais através da divulgação atempada dos dados de tráfego retidos, de forma a responder de forma mais eficaz à persecução de combate aos eventos de cibercrime, que antes não existiam.

O desenvolvimento de tratados e convenções internacionais em matéria penal, particularmente em relação ao cibercrime, permite a integração entre os países com o objetivo de desenvolver regras efetivas para a repressão de crimes. No entanto, mesmo diante da natureza transacional dos crimes cibernéticos, existem mecanismos legislativos e preventivos nacionais que precisam ser aprimorados e aplicados na matéria (BITENCOURT, 2020).

Existe, portanto, a possibilidade de obtenção de dados digitais armazenados fora do território nacional de cada Parte, sendo válidos para o processo, quando tais dados forem públicos, ou seja, de livre acesso de qualquer lugar (código aberto), ou quando houver o consentimento voluntário de quem estaria legalmente autorizado a fornecê-los. Portanto, ou o próprio criminoso deve consentir voluntariamente em fornecer esses dados, ou a empresa provedora de Internet, proprietária desses dados, deve ter uma autorização expressa nesse sentido, o que não parece facilitar o trabalho dos investigadores. No entanto, há casos decididos por tribunais europeus,

americanos e até brasileiros, que têm servido de guia para solucionar essa necessidade de obtenção de provas digitais, que não seriam alcançadas pela jurisdição do país onde a investigação e/ou julgamento está ocorrendo (COSTA, 2021).

3 A IMPORTÂNCIA DA PERÍCIA TÉCNICA EM CRIMES CIBERNÉTICOS

3.1 A PROVA TÉCNICA E SUA RELEVÂNCIA PARA A FORMAÇÃO DO CONVENCIMENTO DO JUIZ EM PROCESSOS CRIMINAIS DE CRIMES CIBERNÉTICOS

Primeiramente, há que se ressaltar que, conforme Paschoal (2015), todo crime provém de uma ação humana. Bitencourt (2020), por sua vez, sustenta que o conceito material de crime possui relevância jurídica, na medida em que se destaca no conteúdo teleológico, determinando, com isso, a razão de constituição de uma conduta humana como infração penal, estando esta, por sua natureza, sujeita à aplicação de sanção. Contudo, segundo o autor, para que se possa considerar determinada conduta como crime, deve haver uma descrição legal (tipificação), sem a qual é impossível atribuir à prática sanção penal.

Neste sentido, relevante é a concepção clássica dada por Jiménez de Asúa (1951 apud MIRABETE; FABBRINI, 2007, p. 82) ao crime, ao determina-lo como sendo a conduta que o legislador considera “[...] contrária a uma norma de cultura reconhecida pelo Estado e lesiva de bens juridicamente protegidos, procedente de um homem imputável que manifesta com sua agressão perigosidade social”. Em complemento, junta-se o conceito dado por Teles (2004, p. 153), que assim expõe:

> [...] para o legislador definir certo fato humano como crime, deve, previamente, verificar se o mesmo é daqueles que lesionam bens jurídicos, ou pelo menos expõem-nos a grave perigo de lesão, e se tais lesões são de gravidade acentuada, de modo a serem proibidas sob ameaça da pena criminal. Do contrário, não poderá o legislador considerá-las crime.

Assim, de um modo geral, pode-se conceber como crime toda conduta que tem vedação expressa pela legislação penal nacional.

Conforme Costa et al. (2021), com o aumento de usuários e a tecnologia em ascensão, os dispositivos eletrônicos e a internet têm se tornado uma poderosa arma na atualidade. Isto porque, ao conectar as pessoas umas às outras, eles também disponibilizam informações sobre elas, que são acessáveis sem burocracia por quem sabe como buscá-las. Isto, contudo, segundo os autores, resulta em algo grave, já que estas informações podem ser utilizadas por criminosos da rede mundial de computadores para fins escusos.

Deste modo, conforme Costa et al. (2021), o que se tem é que, se é verdade que o ciberespaço é um espaço virtual que reduziu fronteiras e aproximou pessoas, formando, a partir daí, uma nova dimensão espacial que proporciona a todos um contato imediato com qualquer pessoa em qualquer parte do mundo em segundos, é certo, também, que se trata de um espaço que proporciona condições para práticas ilícitas, capazes de causar danos às pessoas conectadas. Neste contexto, importante contribuição é dada por Corrêa (2010), que assim define os crimes digitais, também denominados cibernéticos[1]:

> Poderíamos dizer que os ‘crimes’ digitais seriam todos aqueles relacionados ‘as informações arquivadas ou em trânsito por computadores’, sendo esses dados, acessados ilicitamente, usados para ameaçar ou fraudar; para tal prática é indispensável a utilização de um meio eletrônico. Toda sociedade dependente da informação acaba sendo vítima de simples ameaças e até do terrorismo e do vandalismo eletrônicos (CORRÊA, 2010, p. 43).

Contudo, como bem pontuado por Pereira e Oliveira (2019), deve-se considerar que os crimes virtuais, caracterizados pela sua periculosidade e diversidade, geram maior dificuldade para sua comprovação e averiguação, sendo imprescindível a realização de perícia para fins de identificação da autoria do delito.

A perícia forense computacional é área responsável pela investigação de crimes cibernéticos investigando fatos e coletando dados para usar como evidência. Trata-se, pois, da modalidade de perícia criada para combater os crimes cibernéticos, que recorre a métodos e análises destinadas à identificação e coleta de evidências eficientes e comprovadas (PEREIRA; OLIVEIRA, 2019). Em complemento a tais considerações, cite-se que, conforme Costa et al. (2021), em se tratando de crimes cibernéticos, se poderá retirar as evidências de quaisquer dispositivos eletrônicos,

[1] Embora no texto da Lei Carolina Dieckmann a nomenclatura utilizada seja delitos informáticos, para este projeto, bem como na pesquisa que se pretende empreender a partir dele, será utilizada a expressão “crime cibernético” para fazer menção a estes delitos.

discos rígidos, celulares, dentre outros. O trabalho do perito forense computacional é traduzir as informações que forem extraídas de um compilado ou de um depósito eletrônico em um formato inteligível para o ser humano, de modo a torná-las evidências digitais para dar suporte ao processo criminal.

A relevância da perícia forense computacional também é ressaltada por Malaquias (2012) ao destacar que, em razão de se desenvolverem e de terem a sua consumação realizada em ambiente virtual, o que, *a priori*, apontaria para a inexistência física de um sujeito ativo, os crimes cibernéticos são considerados complexos. Costa et al. (2021) dispõem ainda que, para além da complexidade característica deste tipo de crime, tem-se ainda o fato de que as provas de sua ocorrência podem ser facilmente perdidas, modificadas ou destruídas (apagadas da rede), sendo necessário um trabalho técnico especializado de recuperação destas para rastrear a atividade criminosa e o seu agente.

CONCLUSÃO

O presente trabalho visa apresentar um diagnóstico do crime no ambiente digital, principalmente por sua incidência, evolução e técnicas cada vez mais sofisticadas e complexas. Por outro lado, pretendia-se focar na resposta do Estado a esse fenômeno. Em outras palavras, como conter, prevenir ou mesmo mitigar crimes cometidos por meio da Internet.

Em resposta a essa dicotomia, várias leis foram promulgadas e publicadas. Nesse contexto, são citados dois grandes atos legislativos, que são objeto de aprofundamento neste artigo: a lei 12.737/12, “Lei Carolina Dieckmann” e a lei 12.965/14, conhecida como “Marco Civil da internet”.

Não é novidade que o cibercrime continua sendo praticado, vale registrar boas iniciativas para combater esse crime moderno. Exemplo disso é a criação de delegacias especializadas, que capacitam técnicos e utilizam ferramentas e instrumentos destinados a identificar e monitorar em tempo real as infrações mencionadas.

Curiosamente, devido à pandemia, houve um aumento significativo na incidência de crimes cibernéticos e, consequentemente, na aplicação da lei Carolina Dieckmann. No entanto, a referida legislação não se mostrou eficaz, exigindo a criação de um novo diploma legal. Ou seja, em 14 de agosto de 2018 foi promulgada

a Lei 13.709, celebrada como Lei Geral de Proteção de Dados, com base no tratamento de dados pessoais, em meio digital, tanto por pessoas físicas quanto jurídicas, inclusive as de direito público, com o objetivo de proteger os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Os benefícios decorrentes da revolução tecnológica são, portanto, claros, mas as adversidades que acompanham essa evolução não podem ser negadas. Portanto, são necessários mecanismos de prevenção e sistemas de controle da Internet, bem como a redução da impunidade e a imposição de sanções mais severas. Vale lembrar que o delito, cuja sanção é de reclusão de três meses a um ano, não se mostrou suficiente para inibir e reprimir esses crimes, sendo um crime de menor potencial ofensivo, de responsabilidade dos juizados especiais, com possibilidade de conciliação criminal, suspensão condicional do processo e acordo sem procuração. Em outras palavras: sanção leve ou inexistente.

Também pode ser substituído por uma sanção alternativa ou restritiva de direitos. Além disso, é uma conduta que pode causar danos irreparáveis às suas vítimas e prevê uma pequena punição diante de todos os danos causados à vítima.

Todo o tema das provas e investigações que farão parte de todo o processo, dificultando o trabalho e que nem sempre conduz a sanções efetivas, estudando o conceito de crimes virtuais, as ferramentas utilizadas, citando ainda o desfalque e a pedofilia infantil como exemplo, casos que acontecem com muita frequência; a aplicação da sanção nestes casos e as lacunas existentes.

O estudo parte da análise de que a legislação possui falhas na punição dos crimes virtuais, em relação à dificuldade de localização dos criminosos, e a apuração das provas para comprovação do crime. As penas previstas são extremamente brandas, sendo considerado um delito com menor potencial ofensivo, devendo haver a criação de novos tipos de criminosos que possam prejudicar o combate aos crimes, devido às dificuldades de punição, provas e pena mínima em face de toda esta dimensão criminal.

No entanto, no processo evolutivo das normas que visam proteger a garantia do direito fundamental à privacidade, a Lei Carolina Dieckmann define como crime a invasão de aparelho informático alheio, o Marco Civil da Internet considera diferente inviolabilidade das comunicações e informações privadas, e por fim, a lei geral de

proteção de dados prevê os casos ocorridos no tratamento de dados pessoais, protegendo o titular de práticas comerciais abusivas.

Conclui-se que ainda é necessária uma legislação que abranja o uso da Internet no Brasil como um todo e que as lacunas existentes na legislação sejam preenchidas para uma punição efetiva e, consequentemente, para tornar a lei efetiva. Em relação à perícia técnica, tem-se que ela é imprescindível para o deslinde do delito.

REFERÊNCIAS

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal:** Parte Geral. 26. ed. rev. atual. São Paulo: SaraivaJur, 2020.

CORRÊA, Gustavo Testa. **Aspectos jurídicos da internet.** 5. ed. rev. atual. São Paulo: Saraiva, 2010.

COSTA, Amanda Barbosa; et al. A importância da computação forense no combate a crimes cibernéticos. **Revista Ibero-Americana de Humanidades, Ciências e Educação,** v. 7, n. 12, p. 801-814, 2021.

MALAQUIAS, Roberto Antônio Darós. **Crime cibernético e prova:** a investigação criminal em busca da verdade. Curitiba: Juruá, 2012.

MIRABETE, Júlio Fabbrini; FABBRINI, Renato N. **Manual de Direito Penal:** parte geral. 24. ed. São Paulo: Atlas, 2007.

PASCHOAL, Janaina Conceição. **Direito Penal:** Parte Geral. 2. ed. atual. Barueri, SP: Manole, 2015.

PEREIRA, Kamille da Silva; OLIVEIRA, Fabio Machado de. Perícia forense computacional e crimes cibernéticos. **Revista Interdisciplinar Pensamento Científico,** v. 5, n. 2, 2019.