CRIMES VIRTUAIS: A LEI CAROLINA DIECKMANN 12.737/2012 E SEUS EFEITOS NO COMBATE A CRIMINALIDADE VIRTUAL NO BRASIL

BEATRIZ CÁSSIA DA SILVA E SILVA: Radialista, Especialista em Comunicação Empresarial e Marketing, Especialista em Assessoria de Comunicação e Mídias Digitais, Especialista em Gestão de Empresas e Negócios e aluna de graduação no curso de Direito pelo Centro Universitário de Ensino Superior do Amazonas.

PAULO SÉRGIO LIMA DOS SANTOS[1]

(orientador)

RESUMO: O artigo científico traz o presente tema a fim de discorrer sobre os novos tipos de crimes oriundos com o surgimento da internet. A pesquisa mostra que a legislação brasileira tem pouco avançado no combate a esses tipos de crimes. Alguns autores defendem que as mesmas leis aplicadas para defender o cidadão dos crimes praticados na realidade também podem ser aplicadas na vida virtual. Outra corrente, defende ao contrário, mostra deficiência no combate aos novos tipos de crimes e pouco avanço na legislação, que garanta aos usuários menos impunidade e mais efetividade na aplicação da lei. A metodologia aplicada é a dedutiva e dialética, a partir da pesquisa bibliográfica de livros, monografias, artigos científicos entre outras pertinentes. A conclusão é que a legislação brasileira tem pouco avançado no combate essa nova criminalidade. Mesmo após a criação da A Lei Carolina Dieckmann 12.737/2012, muitos são os delitos virtuais que a cada dia emergem e necessitam de aplicação legal que garanta maior punibilidade aos infratores.

Palavras-chave: internet; crimes virtuais; legislação; direito penal; impunidade.

ABSTRACT: The scientific article brings the present theme in order to discuss the new types of crimes arising from the emergence of the internet. The research shows that Brazilian legislation has made little progress in combating these types of crimes. Some authors argue that the same laws applied to defend the citizen from crimes committed in reality can also be applied in virtual life. Another current, argues on the contrary, shows a deficiency in the fight against new types of crimes and little progress in legislation, which guarantees users less impunity and more effectiveness in law enforcement. The methodology applied is deductive and dialectical, based on bibliographic research of books, monographs, scientific articles, among others. The conclusion is that Brazilian legislation has made little progress in combating this new crime. Even after the creation of the Carolina Dieckmann Law 12,737/2012,

[1] Professor Doutor do Centro Universitário de Ensino Superior do Amazonas.

there are many virtual crimes that emerge every day and need legal application that guarantees greater punishment for offenders.

Word-key: internet; cyber crimes; legislation; criminal law; impunity.

INTRODUÇÃO

O tema do presente artigo mostra-se importante, pois com a evolução tecnológica e o surgimento da internet houve significativas facilidades e flexibilidade no tempo das pessoas, tornando o dia a dia das mesmas muito mais proveitoso e produtivo.

Porém, toda vantagem carrega consigo também sua desvantagem. A vantagem da internet é sua facilidade de uso e resolução de problemas virtualmente. Como desvantagem, pode-se citar a vulnerabilidade do usuário diante do uso da rede virtual. E é justamente nessa linha tênue entre vantagem e desvantagem que o criminoso atua, cometendo diversos crimes, antes praticados na vida real e, agora, na vida virtual.

Ante o exposto e no intuito de desvendar o andamento da legislação brasileira perante os crimes virtuais, o tema mostra-se favorável à pesquisa científica, a fim de alcançar o resultado do atual cenário jurídico na esfera virtual.

Por esse motivo, o artigo traz como tema "Crimes Virtuais: A Lei Carolina Dieckmann 12.737/2012 e seus efeitos no combate a criminalidade virtual no Brasil".

Logo, indaga-se: após a criação da "Lei Carolina Dieckmann" houve diminuição dos crimes virtuais?

O objetivo geral é demonstrar se a criminalidade virtual tem diminuído ou aumentado após o advento da Lei 12.737/2012.

Para tanto, foram delineados os seguintes objetivos específicos, os quais serão desenvolvidos ao longo deste artigo: Internet: o surgimento dos crimes virtuais; crimes virtuais: puros e impuros; legislação brasileira x cibercriminalidade; a Lei Carolina Dieckmann 12.737/2012; e impunidade dos crimes virtuais.

Os métodos utilizados são dedutivo e dialético, a partir da pesquisa bibliográfica, aplicada a hipótese sobre o crescente uso da internet e a vulnerabilidade do usuário em face aos crimes virtuais. A pesquisa tem como embasamento teórico livros, monografias, artigos científicos entre outras pesquisas pertinentes.

O artigo traz como hipótese que a evolução tecnológica, como a vivenciamos hoje, carrega consigo tanto vantagens quanto desvantagens. Entre essas desvantagens está a vulnerabilidade das pessoas quanto ao uso da internet, alvos fáceis de crimes virtuais.

Antes, as pessoas tinham que se defender juridicamente dos crimes praticados na realidade. Atualmente, com a realidade da internet, também é necessário se prevenir e se defender de crimes praticados na vida virtual.

Na primeira seção, será discorrido sobre o surgimento dos crimes virtuais na era da internet. Na segunda seção, será especificado quais são esses crimes virtuais e como podem ser classificados. A terceira seção traz um panorama de como a legislação brasileira tem atuado para combatê-los. Em seguida, é realizado o estudo de caso sobre a Lei Carolina Dieckmann 12.737/2012 e a efetividade desta a partir de sua tipificação criminal. E, por último, é explanado como os crimes virtuais causa a sensação de impunidade entre os usuários.

Ao final, conclui-se que a problemática é respondida com a confirmação da hipótese, indicando a necessária adoção de uma legislação própria e mais robusta para combater os crimes virtuais atuais e vindouros, que evoluem paralelamente às novas tecnologias e formas de comunicação em rede.

1 INTERNET: O SURGIMENTO DOS CRIMES VIRTUAIS

Com o advento da internet surgiram inúmeras facilidades para o dia a dia do cidadão, tornando-se um campo fértil para atuação de criminosos, haja vista uma maior exposição do usuário em rede. Ou seja, quanto mais o internauta disponibiliza informações pessoais na internet, maiores tornam-se as opções para a prática de delito virtual. Como exemplifica Moisés de Oliveira Cassanti:

> (...) As pessoas estão cada vez mais conectadas e essa nova realidade social que nos cerca, por um lado, trouxe, sem dúvidas, muitas facilidades e progressos, E por outro, nos deixou mais vulneráveis a riscos inerentes da tecnologia da informação, criando uma nova modalidade de crimes, os chamados crimes virtuais. (CASSANTI, 2014, p. 9)

Os crimes virtuais também são conhecidos por "(...) crimes digitais, informáticos, telemáticos, de alta tecnologia, crimes por computador, fraude informática, delitos cibernéticos, crimes transnacionais, dentre outras nomenclaturas. (...)" (ALBUQUERQUE apud MAUES; DUARTE; CARDOSO, 2018, p. 170).

Enquanto a internet traz inúmeras facilidades, ela também carrega consigo diversas vulnerabilidades, onde o criminoso virtual atua. Ainda segundo Maues, Duarte e Cardoso, "a internet pelo seu uso generalizado e pelo amplo acesso, alavanca riscos oriundos da vulnerabilidade do meio digital, sendo assim, quanto maior a utilização da internet nas interações humanas, mais se potencializa a tendência de surgimento de problemas legais, inclusive, o nascimento de novos tipos de crimes." (MAUES; DUARTE; CARDOSO, 2018, p. 170).

Para Cassanti, essas vulnerabilidades dizem respeito a falta de segurança adequada ao equipamento informático utilizado, como explica:

> Dizemos que um computador é vulnerável quando este apresenta várias deficiências de segurança. Antivírus desatualizado, sistemas operacionais piratas (que não podem receber atualizações), firewall desativado ou configurações incorretas da rede e ainda falhas nos softwares. Os atacantes exploram essas vulnerabilidades, resultando em possíveis ataques e danos para o computador ou seus dados pessoais. (CASSANTI, 2014, p. 21)

A vulnerabilidade dos usuários também está associada ao sentimento de impunibilidade que muitos criminosos sentem, pela internet ainda ser um campo de difícil localização do infrator ou de fácil adulteração de dados relevantes que possam vir a identificá-lo.

2 CRIMES VIRTUAIS: PUROS E IMPUROS

Para alguns autores, os crimes virtuais podem se equiparar aos crimes reais, mudando somente o meio onde o mesmo é praticado, sendo possível a aplicação da legislação vigente. Como enfatiza Diego Cruz e Juliana Rodrigues:

> (...) O que faz as pessoas acharem que há sempre a impunidade nos cybercrimes é o fato das previsões legais não trazerem no preâmbulo o verbo "internet". Ainda que no preâmbulo não traga "internet", o fato dos sujeitos utilizarem a rede como meio de praticar o ilícito, a consumação possui tipificação de modo que podem ser aplicadas as sanções. (CRUZ; RODRIGUES, 2018, p. 6)

Porém, o presente trabalho não irá adentrar essa discussão, mas exemplificar o que são os crimes virtuais. Para Gabrielly Santos:

> Não há uma legislação que trate o conceito de crimes cibernéticos, nem tão pouco que os classifique, as análises e condenações são feitas a partir do Código Penal Brasileiro. No entanto, alguns autores classificam tais crimes como puros e impuros, sendo os puros as condutas não tipificadas e os impuros os tipos penais já tipificados e que ocorrem no ciberespaço. (SANTOS, 2021, p. 11)

Segundo a autora, não há uma legislação que conceitue os crimes virtuais, sendo que sanções são aplicadas consoante a legislação já existente, recebendo a terminologia de puros (ou próprios) e impuros (ou impróprios). Também vale destacar que o Marco Civil da Internet (Lei 12.965/2014) também tem aplicação no Código Penal e Processual Penal.

Os crimes puros ou próprios são os praticados no uso dos meios tecnológicos, emergindo desses como novos crimes virtuais e não como crimes reais praticados no meio virtual. Como explica Barreto e Brasil:

> São aqueles em que os sistemas informatizados, banco de dados, arquivos ou terminais (computadores, smartphones, tablets, por exemplo) são atacados pelos criminosos, normalmente após a identificação de vulnerabilidades, seja por meio de programas maliciosos ou, ainda, por engenharia social (golpista engana a vítima, fazendo com que forneça informações pessoais e/ou estratégicas). (...) (BARRETO; BRASIL, 2016, p. 17)

E os crimes impuros ou impróprios são os já existentes no ordenamento jurídico. Os mais comuns são pornografia infantil, crimes contra a honra, fraudes virtuais, crimes contra a propriedade intelectual e estelionato.

No caso dos crimes impuros a legislação é aplicada por analogia. Diferenciando-se somente o meio onde a prática delitiva é cometida, nesse caso, a internet.

Em relação aos crimes puros existem leis, que foram adaptadas visando abranger esse campo midiático que é a internet. De acordo com Adriano Rocha:

> Além das alterações no Código Penal Brasileiro, que inseriu infrações cibernéticas no bojo da lei através da Lei 12.737/2012, apelidada de "Lei Carolina Dieckmann", temos ainda o ECA (Lei 8.069/90), a Lei de Software (Lei antipirataria no 9.609/98), a Lei de Racismo (Lei no 7.716/89) e a Lei de Segurança Nacional (Lei 7.170/83), compondo o conjunto de normas mais relevantes aplicáveis ao cibercrime. (ROCHA, 2017, p. 18)

Este trabalho abordará especificamente a Lei Carolina Dieckmann (Lei 12.737/2012), a qual será analisada mais adiante.

3 LEGISLAÇÃO BRASILEIRA X CIBERCRIMINALIDADE

Para os autores Cruz e Rodrigues (2018), a dificuldade em punir os cibercriminosos não se encontra na dificuldade de encontrar lei específica, mas na dificuldade de identificá-los e determinar de quem é a competência para julgá-los.

Porém, na doutrina há também quem defenda a criação de uma legislação própria voltada à internet, como defende o autor Paulo Valera:

> Apesar de a tecnologia avançar de maneira desenfreada, o Direito deve adaptar-se a ela. O ambiente virtual tem-se tornado um meio de atuação para o cometimento de crimes, pois se acredita que nele há certa dificuldade para a identificação de quem comete um ato ilícito na internet, por exemplo, o que não é totalmente verdade. (VALERA, 2019, p. 10)

Ou seja, por mais que se tenha uma gama de leis que possam ser aplicadas por analogia, ainda assim, é de suma importância que se tenha uma lei própria, a qual abranja todo e qualquer delito praticado na internet.

Nesse ínterim, Barreto e Brasil também concordam ao afirmarem: "dessa forma, podemos perceber que a lei brasileira não pode nem deve ser excluída da apreciação dessa nova forma de comunicação sem fronteiras, a fim de se evitar a completa anomia, o que poderia gerar para as vítimas a sensação de que a internet é um local no qual tudo se permite." (2016, p. 80).

Atualmente, existe no Brasil o Marco Civil da Internet (2014). Contudo, o mesmo ainda não consegue abranger todo e qualquer delito virtual. A lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil. Para Ana Paula Assunção, apesar das recentes legislações acerca dos crimes virtuais ainda há muito a se fazer, conforme ela:

> Observa-se que destarte tenha ocorrido no passado recente significativos avanços acerca da temática, ainda há muito a se fazer no sentido do aperfeiçoamento normativo em razão da temática se tratar de novidade tanto aos olhos da sociedade quanto ao legislativo, bem como à constante mutação das práticas delitivas nos ambientes virtuais além de a legislação recente estar em fase de teste prático. (ASSUNÇÃO, 2018, p. 21)

Corrobora com Assunção, Maues, Duarte e Cardoso: "A internet, portanto, é um novo caminho para a realização de delitos já praticados no mundo real, sendo necessário que as leis sejam adaptadas para os crimes eletrônicos. Essa é a nova missão da Justiça: adaptar os vários dispositivos do Código Penal no combate ao crime digital." (MAUES; DUARTE; CARDOSO, 2018, p. 177).

E segundo os autores Barreto e Brasil, "(...) apesar de o Marco Civil dispor sobre a possibilidade de exclusão de imagens e vídeos quando publicados, ainda não há lei que trate especificamente sobre o assunto. Apesar disso, a conduta pode ser tipificada como crime contra a honra (adulto) ou contra criança e adolescente, com penalização prevista no ECA." (2016, p.165).

Para os autores Cláudio Bomfati e Armando Kolbe, é urgente a criação de legislação específica para os crimes cometidos na internet. "É incontestável a urgência de uma legislação que esteja muito mais sintonizada com a realidade atual. A justiça brasileira tem conseguido caminhar, ainda que com passos tímidos, diante do crescimento exponencial da internet." (2020, p. 164)

Assim, como é urgente a criação de leis nacionais mais severas que acompanhem a evolução dos crimes no meio virtual, também se faz necessária a cooperação internacional para o combate a esses crimes, haja vista que a internet é um canal de comunicação, a qual interliga as pessoas em todas as partes do mundo. Para as infrações não é diferente, pois a mesma pode ser cometida de qualquer

lugar e/ou de vários lugares em simultâneo. Por isso, a importância da cooperação internacional.

Atualmente, existe a Convenção sobre o Crime Cibernético, também conhecida como Convenção de Budapeste, que entrou em vigor em 2004, pelo Conselho da Europa. Hoje em dia, há a adesão de outros países fora do eixo, a fim de firmarem uma cooperação internacional para os crimes virtuais. E somente após passados 18 anos é que o Brasil tornou-se signatário, com o Decreto Legislativo 37/2021 (AGÊNCIA SENADO, 2021).

4 A LEI CAROLINA DIECKMANN 12.737/2012

Neste trabalho, vamos nos ater a Lei 12.737/2012, apelidada de "Lei Carolina Dieckmann". Esta foi uma das primeiras leis criadas no combate ao crime virtual. Mas antes, se faz necessário entender o caso e por que a lei ganhou o nome da atriz.

Em maio de 2012, a atriz teve, arquivos copiados de seu computador pessoal, 36 (trinta e seis) fotos em situação íntima e conversas, que acabaram divulgadas na Internet sem autorização. Na época, a polícia civil do Rio de Janeiro chegou até 4 suspeitos de terem vazado as fotos e chantageado a vítima a pagar um valor em dinheiro de R$ 10.000,00 (dez mil reais), para as fotos não serem divulgadas (G1, 2012).

O projeto de lei encontrava-se em tramitação desde novembro de 2011, no Congresso Nacional. Porém, somente após o escândalo e o envolvimento de uma figura pública, como a atriz, é que o projeto saiu do papel e passou a ter eficácia como lei. A Lei 12.737/2012 foi publicada no dia 3 de dezembro de 2012 e entrou em vigor no dia 2 de abril de 2013.

A "Lei Carolina Dieckmann" foi criada com a finalidade de criminalizar as condutas cometidas através dos meios informáticos. Segundo Cassanti, "(...) tais como: invasão de computadores, roubo e/ou furto de senhas e de conteúdos de e-mails e a derrubada intencional de sites, inclusive oficiais, o que tem ocorrido em todo o mundo. (...)" (2014, p. 95).

Assim, a lei se enquadra no crime denominado puro ou próprio, consoante as alterações ao Código Penal trazidas pelos artigos 154-A e 154-B. Os artigos tratam de "Invasão de dispositivo informático" e "Ação penal", conforme abaixo:

> **Art. 154-A**. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
>
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.

§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

§ 4º Na hipótese do § 3º , aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:

I - Presidente da República, governadores e prefeitos;

II - Presidente do Supremo Tribunal Federal;

III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia

Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal;

ou

IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou

do Distrito Federal."

Conforme o Artigo 154-A, são vários os requisitos legais que tipicam e materializam a conduta delitiva. No caso da atriz, ela teve o computador pessoal invadido, para obtenção de vantagem financeira, de modo a não ter suas fotos íntimas divulgadas na internet. Logo, conforme o caput, o crime possui pena de detenção de 3 meses a 1 ano mais multa, penalidade esta que pode ter causa de aumento a partir das qualificadoras, chegando a pena de reclusão de até 2 anos.

A segunda alteração no Código Penal foi trazida pelo Art. 154-B, como segue:

> **Art. 154-B**. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos."
>
> Art. 3º Os arts. 266 e 298 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, passam a vigorar com a seguinte redação:
>
> "Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública
>
> Art. 266..
>
> § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
>
> § 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública." (NR)
>
> "Falsificação de documento particular
>
> Art. 298.. ..
>
> Falsificação de cartão
>
> Parágrafo único. Para fins do disposto no caput , equipara-se a documento particular o cartão de crédito ou débito." (NR)

Neste Art. 154-B, o crime virtual alcança também a esfera pública, sendo que a punibilidade é maior e a detenção é de 1 até 3 anos mais multa. O artigo ainda engloba a falsificação de cartão de crédito ou débito, considerando que muitas das transações bancárias atuais ocorrem no meio virtual através da internet e aplicativos de agências bancárias. A pena para este último delito é de reclusão de 1 a 5 anos mais multa.

No caso da atriz Carolina Dieckman, ela foi vítima de uma ciberextorsão, quando, segundo os autores Barreto e Brasil, "(...) verifica-se que os criminosos, mediante grave ameaça - normalmente de divulgar algo que pode expor a vítima à execração pública, trazendo-lhe prejuízos emocionais, sociais, etc. - constrangem as vítimas a pagarem quantias em dinheiro, sob pena de verem vazadas informações íntimas no ambiente virtual." (2016, p. 190).

Em relação aos suspeitos, como ainda não havia lei para crimes informáticos, a Justiça se baseou no Código Penal. Conforme esclarece Bomfati e Kolbe, "presos esses indivíduos (cinco homens, pelo que se divulgou na impressa à época), eles foram indiciados por extorsão, difamação e furto, mas não propriamente por terem invadido o computador da atriz, pois inexistia lei tipificando tal conduta como crime." (2020, p. 63).

Segundo Rocha, "(...) a Lei 12.737/2012 apenas inseriu alguns delitos no Código Penal relacionados aos crimes praticados contra a atriz Carolina Dieckman, mas não abrange toda a gama de condutas delituosas existentes no mundo digital." (2017, p. 14).

Ou seja, a lei tipica alguns dos crimes virtuais, como os praticados contra a atriz, abrangendo ainda os entes públicos e a falsificação de cartão de crédito ou débito. Logo, após a vigência da lei, os crimes virtuais enquadrados por esta, passaram a obter as sanções pertinentes.

Conforme o Art. 154-B, a ação penal é pública condicionada à representação, salvo os crimes cometidos contra a administração pública, quando a ação penal será pública incondicionada. Segundo Maues et al, "(...) trata-se de direito disponível, dependendo de provocação do ofendido. Em razão da disponibilidade do bem jurídico tutelado, o consentimento do ofendido exclui o direito de punir do Estado. No entanto, a ação penal será pública incondicionada se o crime for cometido contra dispositivos da administração pública." (2018, p. 175).

Portanto, quem for vítima de um crime virtual deverá propor ação pública condicionada, manifestando seu interesse pela ação penal. Para isso, é necessário ainda que a vítima reúna todo meio de prova possível, para a identificação da autoria do crime.

Outra ação necessária tanto da vítima quanto da polícia, durante a investigação, é "(...) estar atentas para a volatilidade da evidência, devendo preservá-la o mais rápido possível, não esquecendo de solicitar ao provedor de internet que preserve o conteúdo e os dados de postagem. (...)" (BARRETO; BRASIL, 2016, p.43).

Ainda conforme os autores, alguns provedores de internet possibilitam ao usuário fazer a denúncia na própria página da internet, além da possibilidade de excluir o material infringente, declarando não haver autorização para a publicação de tal material.

5 (IM) PUNIDADE DOS CRIMES VIRTUAIS

Essa sensação de liberdade no meio virtual é sentida tanto por quem pratica o delito quanto pela vítima, pois, segundo os autores Alessandro Barreto e Beatriz Brasil:

> Muitas pessoas, ao se conectarem ao ciberespaço, experimentam a ilusória sensação de liberdade, acreditando

> não estarem adstritas às normas legais, éticas e convenções sociais, pois não estão sendo vigiadas fisicamente por outrem. E esse pensamento, infelizmente, passa não só pela cabeça de criminosos, como também, muitas vezes, pela das vítimas, que desconhecem ou não dão relevância aos riscos que correm no ambiente virtual. (BARRETO; BRASIL, 2016, p. 189)

Para Cláudio Araújo, essa sensação de impunibilidade apresenta a internet como uma terra sem lei. Conforme ele:

> O Código Penal do país faz a tipificação de várias atuações que possuem enquadramento no ambiente web; entretanto, possui penas brandas e sem suficiência para a coibição da prática desses atos. Existe também a lei Carolina Dieckman, que alterou o Código Penal, inserindo artigos em seu corpo. Mas, mesmo da especificação das condutas com prática na web, acaba trazendo dúbias interpretações e punições plácidas para os criminosos. Com isso, a ausência de uma legislação em especificidade ao cybercrime faz a intensificação da ideia de que a internet é uma terra sem lei. (ARAÚJO, 2021, p. 15)

No entanto, para combater a impunidade, Cassanti alerta que a vítima deve se precaver, coletando e salvando todo tipo de evidência que possa ajudar a identificar o cibercriminoso. Como, por exemplo, "imprima e salve arquivos, e-mail, telas, páginas de internet, tudo que possa comprovar o crime. No mundo virtual as evidências podem desaparecer de uma hora para outra." (CASSANTI, 2014, p. 64).

Numa investigação policial, as provas podem ser obtidas primordialmente pelo endereço de IP do usuário. Como explica Bomfati e Kolbe:

> Nas investigações de cybercrimes, entre as diversas evidências que podem ser coletadas, podemos destacar o endereço IP como uma das de maior relevância, pois endereço que proporciona a identificação das conexões entre os computadores, ou mesmo de redes locais com a internet. De maneira simplista, o IP é uma espécie de CPF individual de seu dispositivo. (BOMFATI; KOLBE, 2020, p. 105)

Os autores Barreto e Brasil enfatizam que para conferir confiabilidade das provas é necessário "(...) que sejam coletados e conferidos por quem detenha fé pública - nesse caso, escrivão de polícia ou outro servidor que, por meio de lei própria, tenha esse atributo, ou, ainda, por meio de ata notarial, em cartório de registro de notas." (2016, p. 41).

Um meio eficaz de prova é a ata notarial, como diz Cassanti, "(...) a ata notarial tem força certificante para comprovar a integridade e a veracidade destes

documentos, atribuir autenticidade, fixar a data, hora e existência do arquivo eletrônico." (2014, p.65).

Porém, atrelado aos cuidados que o usuário em rede deve tomar e os cuidados para a preservação de provas de crimes cometidos na internet, deve-se haver um policiamento cibernético intensivo alinhado a legislação existente, a fim de combater a prática ilícita no meio virtual. Consoante os autores Altamiro Favero e Bruno Favero:

> Conforme o exposto conceitua-se o policiamento em ambientes digitais como sendo todas as atividades de prevenção e repressão a infrações penais, desenvolvidas por órgãos de polícia, que sejam voltadas a ciberespaço, ou que se apresentem como adequadas na transição entre os meios eletrônicos e o espaço físico. (FAVERO; FAVERO, 2021, p. 37)

O policiamento ostensivo no ciberespaço é um dos meios mais efetivos para combater a cibercriminalidade e desvirtuar a sensação de impunibilidade nesse campo que é a internet.

No entanto, essa impunibilidade também se deve a falta de preparo policial para lhe dar com esse novo tipo de crime que é o virtual. Como frisa Bomfati e Kolbe:

> Por incrível que pareça, na maioria dos órgãos federais, estaduais, municipais etc. existem ainda agentes despreparados, sem qualquer conhecimento sobre essas novas tecnologias. O desconhecimento dos termos relacionados ao *cybercrime* e das necessidades de uma investigação nesse sentido também são falhas percebidas e, ao final, acabam deixando a sociedade mais vulnerável. (BOMFATI; KOLBE, 2020, p. 166)

Pois, no policiamento cibernético, se faz necessário que as equipes especializadas estejam treinadas e alinhadas para esse trabalho. Já para Maués, Duarte e Cardoso, não somente a polícia precisa estar preparada, mas todo o corpo jurídico nessa empreitada de combate aos crimes virtuais.

> (...) Ou seja, delegacias de polícias precisam ser especializadas em crimes cibernéticos, os juízes devem se atualizarem nas jurisprudências e doutrinas que envolvem delitos informáticos e os advogados, públicos ou privados, devem acompanhar a evolução do Direito Digital para que possa haver uma melhora no funcionamento da Justiça no Brasil. (MAUES; DUARTE; CARDOSO, 2018, p. 178)

Somente assim, será possível combater a impunidade e os delitos cibernéticos. Além de trazer a aplicação da justiça nesse campo fértil de interações humanas e sociais da internet, que a cada dia evolui com as novas tecnologias.

6 MATERIAL E MÉTODOS

Os métodos do artigo são dedutivo e dialético, a partir da pesquisa bibliográfica, aplicada a hipótese sobre o crescente uso da internet e a vulnerabilidade do usuário perante os crimes virtuais. O uso dos métodos busca discorrer sobre o atual cenário da internet e a aplicação da lei cabível para a punibilidade dos crimes praticados na internet.

O método de procedimento adotado é o Monográfico e Estudo de Caso, a partir da Lei Carolina Dieckmann 12.737/2012.

A coleta de dados do artigo foi por pesquisa bibliográfica de livros, monografias, artigos científicos entre outros materiais de estudo pertinentes.

7 RESULTADOS E DISCUSSÃO

Após a repercussão da Lei "Carolina Dieckmann" entre outras legislações voltadas à internet, foi fundada no Brasil, em 2015, a Safernet Brasil, associação de direito privado com atuação nacional, cuja finalidade inicial era desenvolver projetos voltados ao combate da pornografia infantil. Como explana Meneses:

> (...) Fundada em 2015 por professores e pesquisadores com a finalidade primária de desenvolver projetos voltados ao combate à pornografia infantil. Consolidou-se como entidade de referência nacional no enfrentamento aos crimes e violações aos Direitos Humanos na Internet, conquistando assim espaço e respeito inclusive no plano internacional, firmando inclusive acordos de cooperação com instituições governamentais, a exemplo do MPF - Ministério Público Federal. (MENESES, 2019, p. 18-19)

De acordo com Cláudio Araújo, a pornografia infantil está entre os crimes mais frequentes no país. "Dentre os crimes que possuem ocorrência com maior frequência no Brasil, apresentam-se os crimes contra a honra, a divulgação de fotos sem autorização e a pedofilia e a pornografia infantil. (...)" (ARAÚJO, 2021, p. 15)

No entanto, a Safernet já atua em todo o mundo há 16 anos, sendo um importante instrumento de consolidação de dados voltados aos crimes virtuais. Durante esse tempo recebeu mais de 4 milhões de denúncias de 108 países em 6 continentes do mundo.

No Brasil, conforme pesquisa realizada em maio deste ano, foram realizados mais de 35 mil atendimentos. "(...) Ajudou 35.057 pessoas em 27 unidades da federação e foram atendidos 9.558 crianças e adolescentes, 2.420 pais e educadores,

4.468 jovens e 18.611 outros adultos em seu canal de ajuda e orientação." (SAFERNET, 2022).

Segundo os indicadores de atendimentos no Brasil, lideram o ranking de atendimentos: Saúde mental/Bem-estar; Sexting/Exposição íntima; Ciberbullyng e Problemas com dados pessoais.

Conforme os dados, a exposição íntima e a divulgação de fotos sem autorização estão no topo da lista de denúncias para as quais os internautas pedem ajuda.

Figura 1: Indicadores Safernet - Brasil

Figura 2: Indicadores Safernet

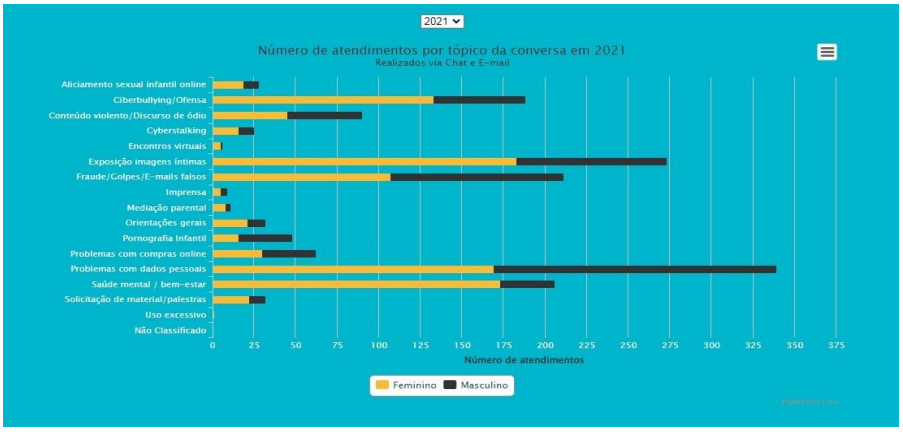

Figura 3: Indicadores Safernet

O que se pode perceber com os tais dados é quão importante é ter legislações que amparem e protejam o cidadão contra qualquer violação de direito fundamental. Pois, segundo o art. 5º, XXXIX da Constituição, "não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal".

Então, foi necessário a repercussão de um caso público como o da atriz Carolina Dieckmann, para que se desse a devida importância aos crimes praticados no mundo virtual e se criasse a Lei 12.737/2012.

De acordo com esta pesquisa, muitos são os crimes virtuais praticados. Porém, a divulgação de imagem íntima lidera os rankings de pesquisa e denúncias, como demonstrado pelos indicadores da Safernet. Este site veio consolidar os crimes virtuais e mostrar os altos índices, que a cada dia crescem mais, pois são registrados e tabulados.

Antigamente, esses indicadores não existiam e ainda não recebiam a devida importância para os delitos oriundos da internet e das novas tecnologias.

Vale salientar que os crimes virtuais são resguardados tanto pela legislação do país quanto pelo Direito Internacional. Como explica Santos:

> Além da legislação nacional, os crimes virtuais também são resguardados pelo direito penal internacional, vez que a

> internet ocorre em escala mundial. Na ceara internacional, a Convenção de Budapeste sobre o cibercrime inovou na forma de cooperação penal e regulamentou formas eficientes de combate aos cibercrimes. A convenção abrange fraudes de informática, violações de direito autoral, pornografia infantil e invasões de computadores. (SANTOS, 2021, p. 31)

Como a internet é um meio que ultrapassa fronteiras, se faz necessário a cooperação internacional para os delitos virtuais e punir os reais infratores que agem em qualquer lugar do mundo, utilizando-se para isso apenas um dispositivo informático conectado à internet.

CONSIDERAÇÕES FINAIS

Dado o exposto, entende-se que com o advento da internet os crimes migraram para um novo cenário que é o digital, com uso de tecnologia e conexão em rede. Nesse ínterim, surge a necessidade de uma nova tipificação criminal para o meio digital, não deixando impune os ilícitos e os infratores que se utilizam desse canal e da fragilidade na legislação para obter vantagens frente as vulnerabilidades dos usuários.

Nesse sentido, o artigo explanou sobre o surgimento dos crimes virtuais, sua classificação em puros e impuros. Porém, destacou os crimes puros, os que se utilizam dos meios tecnológicos para cometer os ilícitos no meio virtual.

Considerando os fatos mencionados, a legislação brasileira apenas deu importância a tipificação desses crimes após reiteradas pressões midiáticas para identificá-los e punir os infratores. Foi o que ocorreu com a Lei Carolina Dieckmann 12.737/2012. Somente após o escandâ-lo com a figura pública da atriz, foi que o Congresso aprovou a lei, a qual passou a vigorar a partir de 2013. No ano seguinte, foi criado o Marco Civil da Internet (2014), visando regular o uso da mesma e minimizar os efeitos danosos causados por seu mal uso.

Mas, mesmo diante de tais regulações, entre outras utilizadas por analogia, como explanado neste artigo, ainda assim, é crescente o número de ilícitos que se valem da conexão em rede.

A medida que esses delitos evoluem, cresce também a sensação de impunidade entre os usuários, haja vista as penas brandas e a fraca regulamentação para detê-los, além também do despreparo de equipes policiais e investigativas para atender os casos.

Conforme dados da Safernet Brasil, em pesquisa realizada no mês de maio, a sexting/exposição íntima está em segundo lugar no topo de atendimentos, perdendo somente para o tópico saúde mental/bem-estar. Ou seja, a criação da Lei Carolina Dieckmann veio a corroborar, estabelecendo um meio de controle para tal ilícito.

Vale ressaltar ainda que a internet é um canal de comunicação que ultrapassa fronteiras, sendo necessária a cooperação internacional no combate aos crimes virtuais que podem ocorrer em qualquer lugar do mundo.

Logo, além de uma legislação nacional mais robusta e com punições mais severas, é preciso também a criação de acordos internacionais, além da Convenção de Budapeste, que agilizem e facilitem a identificação dos infratores virtuais.

REFERÊNCIAS BIBLIOGRÁFICAS

AGÊNCIA SENADO. In.: Senado Notícias. **Congresso ratifica acordo internacional sobre crimes cibernéticos**. Da Redação, 2021. Disponível em: <https://www12.senado.leg.br/noticias/materias/2021/12/23/congresso-ratifica-acordo-internacional-sobre-crimes-ciberneticos>. Acesso em: 28/08/2022.

ARAÚJO, Cláudio Rodrigues. **Análise da aplicação do direito penal nos Crimes Virtuais.** Pensar Acadêmico - ISSN 1808-6136, ISSN on-line 2674-7499, Manhuaçu, v. 19, n. 2, p. 494-511, maio-setembro, 2021.

ASSUNÇÃO, Ana Paula Souza. **Crimes Virtuais**. 2018. 42 f. Trabalho de Conclusão de Curso (Bacharelado em Direito) – UniEvangélica, Anápolis, 2018.

BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de investigação cibernética à luz do Marco Civil da Internet**. - Rio de Janeiro: Brasport, 2016.

BOMFATI, Cláudio Adriano; e KOLBE, Armando Junior. **Crimes Cibernéticos**. Curitiba: Intersaberes, 2020.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Diário Oficial [da República Federativa do Brasil], Brasília, DF, n. 232, 03 dez 2012. Seção I, p. 01-02.

CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais**. - Rio de Janeiro: Brasport. 2014.

CENTRO UNIVERSITÁRIO DE ENSINO SUPERIOR DO AMAZONAS. **Manual do Trabalho de Curso (TC): Graduação em Direito**. Manaus: CIESA, 2022.

CRUZ, Diego; RODRIGUES, Juliana. **Crimes cibernéticos e a falsa sensação de impunidade**. Revista Científica Eletrônica do Curso de Direito – ISSN: 2358-8551, Garça,13ª Edição – Janeiro de 2018.

FAVERO, Altamiro de Oliveira; FAVERO, Bruno de Oliveira. **Cibercriminologia: os meios eletrônicos e o policiamento em ambientes digitais**. - 1. ed. - Jundiaí (SP): Paco Editorial, 2021.

G1. In.: Rio de Janeiro. **Do G1, com informações do Fantástico**. G1, 2012. Disponível em: <https://g1.globo.com/rio-de-janeiro/noticia/2012/05/suspeitos-

do-roubo-das-fotos-de-carolina-dieckmann-sao-descobertos.html>. Acesso em: 23/04/22.

MAUES, Gustavo Brandão Koury; DUARTE, Kaique Campos; CARDOSO, Wladirson Ronny da Silva. **CRIMES VIRTUAIS: Uma análise sobre a adequação da legislação penal brasileira**. Revista Científica da FASETE, p. 166-180, 2018.

MENESES, Sâmia Pereira. **Crimes Virtuais: possibilidades e limites da sua regulamentação no Brasil**. Artigo de Conclusão de Curso (Bacharelado em Direito) – Centro Universitário Fametro – UNIFAMETRO, Fortaleza, 2019.

ROCHA, Adriano Aparecido. **CIBERCRIMINALIDADE: Os crimes cibernéticos e os limites da liberdade de expressão na internet**. 2017. 52 f. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Faculdade de Ensino Superior e Formação Integral, Garça - SP, 2017.

SAFERNET. In.: Datasafer. **35.057 ATENDIMENTOS E 4.441.595 DENÚNCIAS**. Safernet, 2022. Disponível em: <https://indicadores.safernet.org.br/indicadores.html>. Acesso em: 16/05/22.

SANTOS, Gabrielly Daianne Alves. **CRIMES VIRTUAIS: tratamento legal e limitações no combate aos crimes cibernéticos**. 2021. 42 f. Trabalho de Conclusão de Curso (Bacharelado em Direito) – UniEvangélica, Anápolis, 2021.

VALERA, Paulo Vinícius de Carvalho. **Crimes Virtuais e a Legislação Brasileira**. 2019. 59 f. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Centro Universitário Toledo, Araçatuba, 2019.