UNIVERSIDADE ESTADUAL DA PARAÍBA
CAMPUS I - CAMPINA GRANDE
CENTRO DE CIÊNCIAS JURÍDICAS
CURSO DE DIREITO

BRENNO DE SOUSA PEREIRA AMORIM

CRIMES VIRTUAIS: ANÁLISE ACERCA DOS PROBLEMAS DE TIPIFICAÇÃO LEGAL DESSAS CONDUTAS NO DIREITO BRASILEIRO

CAMPINA GRANDE
2019

BRENNO DE SOUSA PEREIRA AMORIM

CRIMES VIRTUAIS: ANÁLISE ACERCA DOS PROBLEMAS DE TIPIFICAÇÃO LEGAL DESSAS CONDUTAS NO DIREITO BRASILEIRO

Trabalho de Conclusão de Curso (Artigo) apresentado ao Curso de Direito da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de Bacharel em Direito.

Área de concentração: Direito Penal

Orientadora: Profa. Dra. Rosimeire Ventura Leite

CAMPINA GRANDE
2019

A524c Amorim, Brenno de Sousa Pereira.
Crimes virtuais [manuscrito] : análise acerca dos problemas de tipificação legal dessas condutas no direito brasileiro / Brenno de Sousa Pereira Amorim. - 2019.
21 p.
Digitado.
Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Estadual da Paraíba, Centro de Ciências Jurídicas , 2019.
"Orientação : Prof. Dr. Rosimeire Ventura Leite , Coordenação do Curso de Direito - CCJ."
1. Direito Penal. 2. Novas tecnologias. 3. Crimes virtuais. I. Título
21. ed. CDD 345

Elaborada por Candice L. Brasileiro - CRB - 15/815 BSCCJ/UEPB

BRENNO DE SOUSA PEREIRA AMORIM

CRIMES VIRTUAIS: ANÁLISE ACERCA DOS PROBLEMAS DE TIPIFICAÇÃO LEGAL DESSAS CONDUTAS NO DIREITO BRASILEIRO

Trabalho de Conclusão de Curso (Artigo) apresentado ao Curso de Direito da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de Bacharel em Direito.

Área de concentração: Direito Penal

Aprovado em: 12/12/2019.

BANCA EXAMINADORA

Profa. Dra. Rosimeire Ventura Leite (Orientadora)
Universidade Estadual da Paraíba (UEPB)

Profa. Milena Barbosa de Melo
Universidade Estadual da Paraíba (UEPB)

Prof. Laplace Guedes Alcoforado de Carvalho
Universidade Estadual da Paraíba (UEPB)

SUMÁRIO

CRIMES VIRTUAIS: ANÁLISE ACERCA DOS PROBLEMAS DE TIPIFICAÇÃO LEGAL DESSAS CONDUTAS NO DIREITO BRASILEIRO

Brenno de Sousa Pereira Amorim[1]

RESUMO

A *internet* é uma ferramenta utilizada pela maioria das pessoas na vida cotidiana e no trabalho, oferecendo amplas possibilidades de interação independentemente da distância. Contudo, para além dos aspectos positivos, a *internet* também se tornou um meio de práticas delituosas, as quais sequer foram imaginadas pelo legislador de alguns anos atrás. Desse modo, o presente artigo tem como objetivo realizar estudo sobre os crimes virtuais, analisando a problemática da tipificação legal de tais delitos no Direito Penal pátrio. Em específico, visa responder questionamentos pontuais, a saber: a legislação penal brasileira está acompanhando as inovações tecnológicas vivenciadas diariamente no tocante aos crimes cometidos virtualmente? E, consequentemente, está o magistrado amparado legalmente para enfrentar tais condutas? Para isso, será realizado breve estudo acerca da evolução da rede mundial de computadores, assim como do Direito Penal pátrio, visando definir qual a melhor solução para o enfrentamento dos crimes virtuais. Justifica-se o tema pela relevância das discussões acerca da repercussão jurídica das condutas praticadas por meio da *internet*. Em relação ao método científico, foi utilizado o método dedutivo, partindo da pesquisa bibliográfica. Visando atender ao seus objetivos, o trabalho realiza exame das correntes doutrinárias majoritárias no Brasil acerca do tratamento dos crimes virtuais, assim como analisa posicionamentos jurisprudenciais que corroboram com a formulação de sua conclusão.

Palavras-chave: Direito Penal. Novas tecnologias. Crimes Virtuais.

ABSTRACT

The internet is a tool used by most people in everyday life and at work, offering wide possibilities for interaction regardless of distance. However, apart from the positives, the internet has also become a means of criminal practices, which could not be imagined by the legislators of a few years ago. Thus, this article aims to conduct a study on cybercrime, analyzing the problematic of the legal typification of such offenses in the homeland criminal law. Specifically, it aims to answer particular questions, namely: is Brazilian criminal law following the technological innovations experienced daily in relation to crimes committed virtually? And, consequently, is the magistrate legally protected to face such conducts? For this, a brief study will be carried out about the evolution of the world wide web, as well as the country's Criminal Law, in order to define what is the best solution to face virtual crimes. The theme is justified by the relevance of the discussions about the legal repercussion of the criminal practices committed through the internet. Regarding the scientific method, the deductive method was used, starting from the bibliographical research. Aiming to meet its objectives, the paper examines the majority doctrinal currents in Brazil about the treatment of cybercrimes, as well as analyzes jurisprudential positions that corroborate to the formulation of its conclusion.

Keywords: Criminal Law. New technologies. Cybercrimes.

---

[1]Graduando em Direito pela Universidade Estadual da Paraíba.

1 INTRODUÇÃO

A *internet* é, nos dias de hoje, uma ferramenta cotidiana que a maioria das pessoas utiliza no seu dia-a-dia, através de computadores, *smartphones*, *tablets*, etc. Ela oferece um acervo de informações instantâneas de enorme magnitude, estando tudo apenas à distância do clicar de um botão. Além disso, a *internet* nos trouxe também uma conectividade inimaginável previamente, sendo possível, através dela, nos comunicarmos com outros usuários nos lugares mais remotos do planeta.

Essa ferramenta trivial da nossa vivência hodierna, porém, pode também ser utilizada para fins lesivos à sociedade e simplesmente criminosos, que é o caso dos crimes cibernéticos (ou virtuais). Estes crimes tratam-se de uma dinâmica relativamente nova no Direito Penal como um todo, sendo seguro afirmar que os legisladores responsáveis pelo Código Penal brasileiro do ano de 1940, por exemplo, não imaginariam a possibilidade da existência de um conglomerado de redes que promovem a interconexão de máquinas eletrônicas em um nível mundial, tampouco delitos que poderiam ser cometidos através dela.

O presente artigo tem por objetivo realizar estudo sobre os crimes virtuais, analisando a problemática da tipificação legal de tais delitos no Direito penal pátrio. Visa, assim, responder questionamentos pontuais, a saber: a legislação penal brasileira está acompanhando as inovações tecnológicas vivenciadas diariamente no tocante aos crimes cometidos virtualmente? E, consequentemente, está o magistrado amparado legalmente para enfrentar tais condutas?

É inegável a relevância social e jurídica do estudo, já que o crime, em sua concepção material, trata-se da conduta que ofende um bem juridicamente tutelado, sendo assim merecedora de pena. Dessa maneira, é necessário fazer valer as garantias fundamentais inerentes a todas as pessoas, que podem vir a ser violadas através das condutas delituosas, nos quais incluem-se as praticadas virtualmente. Ademais, o grande crescimento da incidência desses crimes virtuais com o passar dos anos chama a atenção, além da sua grande incidência no Brasil, que está entre os cinco países com mais crimes virtuais no mundo, causando uma reflexão acerca das formas de combatê-los no nosso país. Sabendo que o Direito é o espelho da sociedade, devendo ele evoluir conforme a sociedade se desenvolve, faz-se necessário notar se a legislação penal do nosso país está atualizada e pronta para enfrentar os casos de crimes cibernéticos.

Após a delimitação do problema a ser trabalhado, quanto ao método científico utilizado, foi adotado o método dedutivo para a construção lógica do raciocínio aplicado no estudo. Já em relação ao tipo de pesquisa utilizado para pautar o trabalho científico, quanto ao meio de investigação, a pesquisa ocorreu de maneira bibliográfica, sendo desenvolvida com base em materiais publicados em livros, artigos científicos, revistas e jornais especializados, isto é, em material de acesso público.

Visando uma boa organização do trabalho a ser apresentado, foi realizada sua divisão em cinco seções, que buscam uma delimitação satisfatória entre os seus temas, intituladas, respectivamente: *Internet*: surgimento e evolução; Direito Penal e os crimes virtuais; Caso Carolina Dieckmann e suas consequências na legislação penal brasileira; A problemática da tipificação dos crimes virtuais na legislação pátria e suas possíveis soluções; e, por fim, Exposição jurisprudencial prévia à Lei 12.737/2012.

Primeiramente, serão feitas breves considerações históricas acerca do advento da rede mundial de computadores, além de expostos pontos importantes que demonstram sua constante evolução até alcançar o que conhecemos como *Internet* atualmente.

Em seguida, elege-se necessário apresentar alguns conceitos básicos do Direito Penal a fim de contextualizar o tema a ser abordado mais a frente, ademais, serão explicados os crimes virtuais e suas classificações, da maneira que são tratados pela doutrina.

Na terceira seção, será mostrado o "caso Carolina Dieckmann", como ele foi enfrentado à época e qual a sua repercussão no ordenamento jurídico brasileiro, analisando as leis especializadas em crimes cibernéticos editadas após tal acontecimento, assim como será exposta brevemente a existência de uma previsão, na forma de convenção internacional existente desde o ano de 2001, da ameaça que tais crimes, cometidos através das novas tecnologias, possuem.

Na quarta parte serão mostrados os dois pensamentos doutrinários majoritários no país acerca da tipificação dos crimes virtuais, que visam solucionar o grande problema da necessidade (ou falta dela) de tipificação dos crimes virtuais no Direito Penal brasileiro.

Por fim, visando ilustrar faticamente a discussão existente, serão apresentados e analisados posicionamentos jurisprudenciais anteriores à edição da Lei 12.737/2012, no que diz respeito ao julgamento de casos atrelados diretamente aos crimes virtuais.

2 INTERNET: SURGIMENTO E EVOLUÇÃO

A informática, segundo Benjamim Loveluck (2018, p. 41), trata-se da "tradução técnica de princípios de organização e de processamento da informação, baseados na digitalização". Sendo assim, destaca-se como a base para toda e qualquer ciência relacionada à coleta, armazenamento, transmissão e processamento de informações em meios digitais, como a ciência da computação e o sistema de informações. Utilizando-se dessa base, os computadores surgiram ainda no século XX, sendo o primeiro computador digital eletrônico criado no ano de 1946, porém, não passava ele de uma enorme máquina de calcular - nada parecido com o que entendemos por computador nos dias de hoje.

Foi durante a Guerra Fria, décadas depois do surgimento de tal máquina, que foram dados os primeiros passos para a invenção da *internet*. Em tal época, marcada pela disputa bélica e tecnológica entre os gigantes Estados Unidos e União Soviética, qualquer triunfo era visto como um passo à frente na disputa pela dominação mundial. Como explica Loveluck:

> As origens imediatas da *internet* são, portanto, o resultado da Agência Arpa (*Advanced Research Projects Agency*), criada em 1958 pelo Departamento de Defesa dos Estados Unidos para coordenar os esforços de pesquisa, após o vexame infligido pelos russos, em 1957, com o lançamento dos primeiros satélites *Sputnik*; estes tiveram o efeito de um eletrochoque, destilando a ideia do atraso da tecnologia dos Estados Unidos e desencadeando um processo de remobilização da pesquisa norte-americana [...] (LOVELUCK, 2018, p. 45).

Foi essa agência americana que criou a ARPANET, como esclarece Nilton Kleina (2011), a ARPANET foi criada como uma rede de armazenamento de dados, a qual, em um primeiro momento teve por objetivo conectar universidades e centros de pesquisa norte-americanos de grande importância no contexto da Guerra Fria. Foi durante as décadas seguintes, que a rede supracitada foi ganhando forma, primeiramente com um novo nome - *internet*; e foram, assim, estabilizadas as suas bases e conceitos básicos.

Porém, fica o questionamento sobre como essa rede de armazenamento de dados, criada num contexto militar, se tornou o que é hoje em dia. Essa evolução aconteceu de maneira gradativa e existem diversos acontecimentos que podem ser indicados como pontos cruciais para tal, a maioria destes, ocorridos na década de 1970. O primeiro a ser citado é o surgimento do correio eletrônico (*email*), idealização de Ray Tomlinson no ano de 1971. Como explana Nilton Kleina (2011), é verdade que já existia um sistema de transmissão de mensagens na ARPANET, porém, esta acontecia apenas entre o mesmo computador, faltando um sistema de comunicação praticamente instantânea entre máquinas dentro de uma rede, criado, assim, por Tomlinson.

O acontecimento mais importante dos anos 70, no que diz respeito à *internet*, é, porém, a criação do TCP/IP (*Transmission Control Protocol / Internet Protocol*). Segundo Ian Peter (2003), o TCP/IP é a espinha dorsal, o protocolo que define o que é a *internet*, ele foi desenvolvido para resolver a problemática da comunicação entre computadores diferentes situados sob a mesma rede (ARPANET), sendo o protocolo usado até os dias atuais. Adiciona Loveluck (2018), que a implementação desse novo protocolo veio a garantir a comunicação com outras redes independentes, fazendo com que as noções de abertura e descentralização, pilares das redes virtuais, assumissem todo o seu sentido. O detalhe que escancara o quão essencial foi a criação desse protocolo para a evolução da *internet*, é que, mesmo depois de quase meia década de seu surgimento, ainda é ele o protocolo padrão utilizado para a transmissão de dados hoje em dia.

Finalmente, foi durante o início da década de 1980 que começou a rápida expansão do uso dos computadores pessoais. Durante esses anos, mudou-se o panorama de utilização de computadores, sendo popularizado seu uso por pessoas comuns, como expõe Benjamin Loveluck (2018, p. 62), "Os usuários não se limitavam a constituir um círculo restrito de cientistas e engenheiros, mas também de estudantes e entusiastas [...]". Foi também no começo dessa década que se observa o crescimento de grandes empresas do ramo tecnológico, como a *Microsoft* e a *Apple*, que ajudaram a ditar a evolução da nova era da tecnologia. Tal evolução não cessou, chegando até os dias atuais, a *internet* continua em constante evolução, agora com um contexto distinto ao em que foi criada: a guerra.

3 DIREITO PENAL E OS CRIMES VIRTUAIS

Em um primeiro momento, resta importante explanar alguns conceitos básicos do Direito Penal que serão essenciais para o presente trabalho. Quanto ao crime em si, destaca o Decreto-lei nº 3.914, de 1941, também conhecido como Lei de introdução do Código Penal, em seu artigo 1°:

> Art 1º Considera-se crime a infração penal que a lei comina pena de reclusão ou de detenção, quer isoladamente, quer alternativa ou cumulativamente com a pena de multa; contravenção, a infração penal a que a lei comina, isoladamente, pena de prisão simples ou de multa, ou ambas, alternativa ou cumulativamente.

Importante notar, porém, que, ao contrário das legislações anteriores, o conceito legal de crime não está expresso no Código Penal brasileiro vigente.

Guilherme de Souza Nucci (2015, p. 119-124) traz em sua obra conceituação de crime sobre três prismas distintos: o material, o formal e o analítico. O primeiro deles, segundo o autor, é conceito aberto e informa o legislador sobre as condutas que merecem ser transformadas em tipos penais incriminadores. Materialmente, o crime é toda conduta merecedora de pena por ofender um bem juridicamente tutelado. Temos então, que se trata de uma ideia anterior à legislação, oferecendo ao legislador um critério sobre o que deve ser punido.

O conceito formal, de maneira distinta, é a concepção do Direito acerca da conduta, proibindo-a por lei sob ameaça de pena, seja qual for. Por fim, segundo o conceito analítico, o crime, como disciplina Nucci:

> Trata-se de uma conduta típica, antijurídica e culpável, vale dizer, uma ação ou omissão ajustada a um modelo legal de conduta proibida (tipicidade), contrária ao direito (antijuridicidade) e sujeita a um juízo de reprovação social incidente sobre o fato e seu autor, desde que existam imputabilidade, consciência potencial de

> ilicitude e exigibilidade e possibilidade de agir conforme o direito (NUCCI, 2015, p. 121).

Temos assim, a definição e exposição da corrente majoritária no Brasil e no exterior acerca da definição do crime sob seu ponto analítico, conhecida como teoria tripartida do crime.

O Direito Penal, assim como os outros ramos do Direito, possui diversos princípios norteadores próprios essenciais para sua existência e correta aplicação na vida em sociedade. É possível afirmar, porém, que o mais importante entre eles se trata do princípio da legalidade, consagrado na Constituição da República Federativa do Brasil de 1988, que, em seu artigo 5º, inciso XXXIX, disciplina não haver crime sem lei anterior que o defina, nem pena sem prévia cominação legal.

Acerca do mesmo, observa Guilherme de Souza Nucci (2015, p. 43): "[...] é a impossibilidade de se considerar criminosa determinada conduta se esta não for considerada lesiva a um interesse juridicamente protegido, merecedora de pena, desde que esteja devidamente prevista em lei". Compartilhando de mesmo entendimento, detém o princípio da legalidade quatro funções fundamentais, de acordo com Greco:

> 1) proibir a retroatividade da lei penal (*nullum crimen nulla poena sine lege praevia*);
>
> 2) proibir a criação de crimes e penas pelos costumes (*nullum crimen nulla poena sine lege scripta*);
>
> 3) proibir o emprego de analogia para criar crimes, fundamentar ou agravar penas (*nullum crimen nulla poena sine lege stricta*);
>
> 4) proibir incriminações vagas e indeterminadas (*nullum crimen nulla poena sine lege certa*). (GRECO, 2015, p. 146)

Fica clara, desse modo, a essencialidade deste princípio não só para moldar o Direito Penal brasileiro, mas também para garantir o seu adequado funcionamento, sendo a partir dele extraído a máxima "tudo que não é proibido, é permitido", no âmbito Penal.

Feitas essas considerações, passa-se ao estudo dos crimes virtuais em específico. Importante fazer uma breve ressalva quanto à nomenclatura utilizada. Não há na doutrina pátria um termo específico uniformizado para tratar os crimes cometidos na área informática, sendo possível chamá-los de crimes virtuais, cibernéticos, informáticos, entre outras denominações. Desse modo, o trabalho não fará distinção entre os termos, utilizando-os como sinônimos. Disciplinam Furlaneto Neto e Guimarães:

> Delito eletrônico, em sentido amplo, é qualquer conduta criminógena ou criminal em cuja realização haja o emprego da tecnologia eletrônica como método, meio ou fim e, em um sentido estrito, qualquer ato ilícito penal em que os computadores, suas técnicas e funções desempenham um papel como método, meio ou fim. (FURLANETO NETO; GUIMARÃES, 2003, p. 70)

Percebe-se, através da definição trazida pelos autores, ao abordarem o uso da tecnologia de três maneiras diferentes (método, meio ou fim), que nem todos os crimes cometidos virtualmente apresentam as mesmas características. Por esse motivo, os doutrinadores elegeram a necessidade de classificar os crimes virtuais. A primeira delas se dá em crimes virtuais puros, mistos e comuns.

Acerca dos primeiros, Marco Aurélio Rodrigues da Silva (1997) disciplina: "são aqueles em que o sujeito ativo visa especificamente ao sistema de informática, em todas as suas formas". Os mistos, porém, continua Marco Aurélio Rodrigues da Silva (1997) "são todas aquelas ações em que o agente visa a um bem juridicamente protegido diverso da informática, porém, o sistema de informática é ferramenta imprescindível a sua consumação". Por fim, os comuns nas palavras de Reginaldo César Pinheiro (2000) "são pois, assim entendidos, porque utilizam a *Internet* apenas como instrumento para a realização de um delito já tipificado pela lei penal pátria".

A classificação mais utilizada doutrinariamente, contudo é outra, mais simples, mas em relativa conformidade com a anterior. Trata-se na diferenciação entre crimes virtuais próprios e impróprios.

Os denominados impróprios, como ressalta Túlio Lima Vianna (2003, p. 37), "são aqueles nos quais o computador é usado como instrumento para a execução do crime, mas não há ofensa ao bem jurídico inviolabilidade da informação automatizada (dados)". Nestes casos, o crime digital é utilizado com o auxílio do computador e/ou *internet*, porém, tal crime já é tutelado, não sendo a máquina estritamente necessária para sua consumação. Destacam-se nessa classificação os crimes contra a honra (calúnia, difamação, injúria), que podem ser cometidos virtualmente, contudo, não só dessa maneira.

Já os próprios, segundo Túlio Lima Vianna (2003, p. 40), "são aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados)". Sendo assim, nos crimes virtuais próprios, o computador/*internet* é meio necessário para a concretização do crime. Se não houver a utilização desses meios, não será possível cometer o delito, existindo, portanto uma relação de essencialidade entre o computador e a realização delitiva. Destacam-se, entre eles, a supressão de dados virtuais e documentos digitais e o dano informático. Porém, ao contrário dos crimes virtuais impróprios, não existem disposições prévias no Código Penal brasileiro que se apliquem à maioria destes, o que leva à noção da necessidade de edição de legislação específica capaz de tipificar especificamente tais condutas, visando preencher a lacuna existente no ordenamento jurídico pátrio.

4 CASO CAROLINA DIECKMANN E SUAS CONSEQUÊNCIAS NA LEGISLAÇÃO PENAL BRASILEIRA

No ano de 2012, a atriz brasileira Carolina Dieckmann foi vítima de *hackers* que acessaram seu computador pessoal através da *internet* e obtiveram fotografias íntimas suas. Além da invasão e obtenção de tais fotos, o grupo chantageou a atriz por cerca de um mês através de *emails*, pedindo a quantia de R$10.000,00 (dez mil reais) para que elas não fossem divulgadas, como informou o advogado da atriz Antônio Carlos de Almeida Castro em entrevista ao G1 na época. Com a recusa da vítima em ceder à chantagem, o grupo realizou a divulgação indevida do material obtido.

Os criminosos utilizaram uma técnica chamada "*phishing*", que visa buscar informações confidenciais de determinada pessoa, além de dados pessoais e bancários, chegando ao seu objetivo através de *emails* falsos contendo links corrompidos. Como explana Fruhlinger:

> *Phishing* é um ataque cibernético que usa um *email* disfarçado como arma. O seu objetivo é enganar o destinatário do *email*, fazendo-o acreditar que a mensagem é algo que ele procura ou precisa - uma mensagem do seu banco ou de um

> companheiro de trabalho, por exemplo - e clicar em um link ou realizar o *download* de um anexo. (FRUHLINGER, 2019, s.p., tradução nossa). [2]

A situação vivida por Carolina Dieckmann não foi, contudo, a primeira vez que se observou um crime virtual deste tipo, já existindo, ao tempo do caso em questão, diversas vítimas registradas em casos semelhantes. Como mostra Neto, no ano de 2009 o FBI (*Federal Bureau of Investigation*), serviço de segurança dos Estados Unidos, prendeu 59 pessoas envolvidas em fraudes virtuais, que, através de *emails* se passando pelo *Bank of America* e o *Wells Fargo*, invadiam as contas bancárias das vítimas e transferiam o dinheiro para contas próprias, conseguindo arrecadar dois milhões de dólares americanos durante os três anos que realizaram as fraudes.

Porém, apesar de não ser uma novidade no espectro mundial, foi o caso da atriz que chamou a atenção da mídia e da sociedade brasileira como um todo, devido a vítima ser uma figura pública com constante atenção midiática. No caso em questão, os envolvidos foram indiciados por furto, extorsão qualificada e difamação, tipificados todos no Código Penal Brasileiro, já que o Brasil não detinha, à época, lei específica destinada a tipificar qualquer conduta praticada no âmbito cibernético, fato que evidenciou o total despreparo do ordenamento jurídico brasileiro para enfrentar a nova ameaça dos crimes virtuais.

Tendo isso em vista, ainda no ano de 2012 foi editada a lei 12.737, intitulada pela imprensa "Lei Carolina Dieckmann", dispondo sobre a tipificação de condutas delituosas no âmbito cibernético e originando oficialmente o crime de "invasão de dispositivo informático", ao acrescentar os artigos 154-A e 154-B ao Código Penal Brasileiro, juntando-os à seção IV do Código, que trata dos "crimes contra a inviolabilidade dos segredos". O artigo 2º da lei diz:

> Art. 2º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:
> "Invasão de dispositivo informático
> 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

---

[2] *Phishing is a cyber attack that uses disguised email as a weapon. The goal is to trick the email recipient into believing that the message is something they want or need — a request from their bank, for instance, or a note from someone in their company — and to click a link or download an attachment.*

> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal."
> "Ação penal
> 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."

Ao analisar os dispositivos criados, nota-se a preocupação do legislador em promover a proteção de possíveis informações sensíveis do proprietário de determinado dispositivo informático, visando o resguardo da sua intimidade e privacidade. O *caput* do artigo 154-A esclarece que a invasão será criminosa se feita para adquirir, alterar ou destruir os dados protegidos pela vítima. O sujeito ativo do crime de invasão de dispositivo informático poderá, dessa maneira, ser qualquer indivíduo que não possui autorização expressa ou tácita do proprietário do dispositivo para o acesso das informações nele contidas. Enquanto o sujeito ativo poderá ser qualquer pessoa proprietária de dados informáticos, que não devam ser de conhecimento público, acessados indevidamente.

O parágrafo 1º do artigo traz determinação de grande importância, prevendo que incorrerá à mesma pena "quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta", estendendo claramente a aplicação do dispositivo não só a quem comete o ato de acesso, adulteração ou destruição dos dados, mas também a quem produz programas informáticos que possibilitam tais ações. O artigo 154-B, por sua vez, tem por finalidade tratar do rito específico do crime supracitado, sendo ele condicionado à representação da vítima nos casos comuns. A lei 12.737/12 ainda traz em seu artigo 3º alterações a dois diversos artigos do Código Penal, que, porém, não são incumbidos de grande relevância ao trabalho.

Apesar do óbvio avanço trazido pela lei, sendo ela a primeira do ordenamento jurídico brasileiro a tratar do assunto satisfatoriamente, a mesma não foi imune à críticas, existindo dois pontos principais abordados por alguns autores ao tempo de sua publicação como vícios importantes. A primeira delas diz respeito à "violação indevida de mecanismo de segurança".

Isso acontece porque a maneira que foi editada o *caput* leva ao entendimento que só poderá ser considerado o crime de invasão de dispositivo informático caso o invasor, para consolidar o ato delitivo, necessite ultrapassar barreiras de segurança previamente impostas pelo proprietário do dispositivo, à exemplo de programas antivírus ou arquivos protegidos por senhas de acesso. Ora, um usuário de aparatos tecnológicos inexperiente, por exemplo, que pode não ter o conhecimento necessário para realizar tais medidas de segurança, não restaria amparado pelo dispositivo legal caso tivesse suas informações privadas invadidas, devido a inexistência dos "mecanismos de segurança".

Em conformidade com esse entendimento, ao fazer comentários sobre o projeto de lei nº 84/1999 (que será abordado mais adiante), que visava tipificar crimes informáticos e possuía a mesma ideia de restrição de acesso mediante violação de segurança, explanou Vianna:

> Não menos absurda é a necessidade de uma "expressa restrição de acesso". O fato de alguém deixar seu *notebook* na mesa de um restaurante enquanto vai ao banheiro, não torna lícita a conduta de quem se aproveita desta ausência para acessar os dados. Não é razoável exigir que o proprietário tenha que declarar expressamente que ninguém está autorizado a acessar seus dados. (VIANNA, 2009, s.p.)

A segunda crítica diz respeito às penas impostas para o crime trazido pela lei 12.737/12: detenção de três meses a um ano e multa, na sua modalidade comum, existindo a possibilidade de aumento de pena de acordo com os parágrafos do artigo 154-A. Na opinião

de Silveira, Sousa e Melo (2017), tratam-se de previsões muito brandas, que não obterão sucesso na premissa de inibir os *hackers* à prática do delito.

A iminência da utilização de dispositivos eletrônicos não era, porém, algo estranho aos operadores do Direito na esfera internacional, algo que os pegou desprevenidos. Prova disso é a Convenção de Budapeste, que foi criada no ano de 2001 pelo Conselho da Europa e entrou em vigor em 2004, servindo como uma espécie de lei mundial sobre os crimes na web. Gills Lopes Macêdo Souza e Dalliana Vilar Pereira elucidam (2009, p. 05): "A convenção prioriza uma política criminal que visa proteger a sociedade contra os *cybercrimes*, através de legislação adequada e da cooperação internacional". O Brasil não é, contudo, signatário desta convenção.

Além da lei 12.737/12 apresentada acima, também faz-se necessário expor a existência de outra lei, sancionada no dia 30 de novembro de 2012 - mesma data da lei "Carolina Dieckmann", que visou trazer algumas determinações relacionadas aos delitos virtuais, a Lei 12.735/2012, chamada de "Lei Azeredo", proveniente do projeto de lei número 84 de 1999, que passou mais de uma década em trâmite, sendo alvo de diversas discussões e alterações ao seu corpo. É importante afirmar que apesar destas inúmeras discussões, segundo Camila Requião Fentanes da Silva (2013), foi o apelo midiático proporcionado pelo caso da atriz brasileira que levou a lei 12.735 a ser sancionada, juntamente à lei 12.737. No final das contas, ao tempo que foi sancionada, os únicos artigos da "Lei Azeredo" que trazem mudança à legislação leem:

> Art. 4º Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.
> Art. 5º O inciso II do § 3º do art. 20 da Lei nº 7.716, de 5 de janeiro de 1989 , passa a vigorar com a seguinte redação:
> "Art. 20. .....
> .....
> § 3º .....
> .....
> II - a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio;
> ....." (NR)

Percebe-se que tais determinações, além de poucas, não atacam efetivamente o problema dos crimes virtuais, o objetivo original do projeto de lei 84/99. Isso acontece porque, diversos dispositivos de tal projeto eram eivados de vícios, que propiciaram as tão longas discussões e resultaram na redução da redação original, que continha 23 artigos, para quatro, dos quais dois deles foram vetados pela então Presidente Dilma Rousseff. Resumidamente, tamanha redução dos dispositivos originais aconteceu, nas palavras de Gills Lopes e Dalliana Vilar (2009, p.8), "face ao desrespeito evidente aos direitos fundamentais e às liberdades civis que aquele acarreta, é explícita a dissonância entre esses instrumentos normativos, bem como a inconstitucionalidade de dispositivos do projeto em análise". Por essas razões, o projeto de lei em questão chegou até a ser intitulado de "AI-5 Digital" por parte dos usuários da *internet*, em clara alusão ao decreto emitido no sombrio tempo da ditadura militar no nosso país.

Considerando o exposto, nota-se que o caso Carolina Dieckmann foi um verdadeiro divisor de águas no que diz respeito à legislação penal pátria, chamando a atenção popular para o grande perigo atrelado ao uso das novas tecnologias. O caso foi de grande importância para o ordenamento jurídico brasileiro, por motivar a publicação de leis específicas para enfrentar os crimes virtuais, embora essas determinações estejam longe da perfeição, como mostrado.

5 A PROBLEMÁTICA DA TIPIFICAÇÃO DOS CRIMES VIRTUAIS NA LEGISLAÇÃO PÁTRIA E SUAS POSSÍVEIS SOLUÇÕES

Diante do exposto acerca dos crimes virtuais na legislação brasileira, é possível levantar algumas indagações: primeiramente, sabendo que o arcabouço legal que trata dos crimes cibernéticos é escasso e as leis que existem são incompletas e imperfeitas, como deverá o magistrado penal agir para enfrentar essa modalidade criminosa satisfatoriamente sem o devido suporte da legislação? Além disso, será que é realmente necessária a edição de leis específicas acerca do assunto, ou existem outras alternativas que possibilitem a luta contra os crimes virtuais, mesmo que, até o presente momento, não os sejam tipificados no nosso ordenamento jurídico?

Tais questionamentos podem ser respondidos de duas maneiras distintas, defendidas por duas principais correntes doutrinárias concorrentes. Uma delas acredita que o problema só será sanado com a edição de leis específicas que tipifiquem todos os crimes virtuais próprios; enquanto a outra prega pela desnecessidade da existência de tais leis, apontando para outras ferramentas legais a serem utilizadas pelos magistrados penais a enfrentar os crimes virtuais.

5.1 TIPIFICAÇÃO DOS CRIMES VIRTUAIS

Primeiramente, é necessário deixar claro que a tipificação defendida por essa corrente não é a de todos os crimes que possam ser cometidos utilizando-se da tecnologia, visto que, como explica Carneiro:

> Quando levantamos a questão da tipificação dos crimes virtuais no ordenamento jurídico brasileiro, pensamos logo em precariedade, mas muitos não sabem que a legislação brasileira alcança de 90 a 95% dos crimes praticados no âmbito virtual em nosso país, pois os crimes praticados por meio do computador para realização do delito, mais conhecidos como a modalidade de crimes impróprios, são normalmente já tipificados em nosso Código Penal. (CARNEIRO, 2012, s.p.)

Como explana a autora, a grande maioria dos crimes cometidos virtualmente já foram previstos na legislação pátria, a exemplo dos crimes de calúnia, difamação e injúria, já tipificados no Código Penal Brasileiro e que podem, ou não, ser cometidos mediante o uso de dispositivos tecnológicos. O problema resta exatamente nos referidos 5% finais não abordados no nosso ordenamento jurídico, que dizem respeito aos crimes virtuais próprios, a exemplo do dano informático.

De acordo com os defensores do presente entendimento, a edição de legislação específica para enfrentar os crimes próprios cometidos através das novas tecnologias é essencial, com base no princípio constitucional da legalidade no Direito Penal (ou princípio da reserva legal), já tratado anteriormente. Acerca dele, observa Guilherme de Souza Nucci (2015, p. 43): "[...] é a impossibilidade de se considerar criminosa determinada conduta se esta não for considerada lesiva a um interesse juridicamente protegido, merecedora de pena, desde que esteja devidamente prevista em lei".

É sabido que uma das funções deste princípio constitucional é exatamente proibir a utilização da analogia *in malam partem*, de acordo com ele, então, como assinala Dayane Fanti Tangerino (2016), "não seria possível, portanto, considerar típico o dano a dados informáticos ou o furto informático, por exemplo, sendo necessária a alteração legislativa penal ou a criação de novos tipos penais que abarcassem estas condutas".

No tocante à possível aplicação do artigo 163 do Código Penal Brasileiro, que tipifica o crime de dano, ao dano informático, crime virtual próprio, diz Marcelo Xavier De Freitas Crespo (2011, p. 72-73, *apud* TANGERINO, 2016) que o espírito da lei, quando o legislador tipificou o artigo 163 do Código Penal, não era o de incluir o dano de dados informáticos,

pois à época não se poderia cogitar o que viria a acontecer, já que os computadores eram pouco acessíveis às pessoas em geral, pelo que, “coisa”, para o nosso Código Penal é bem tangível, sendo assim, seria necessário alterar a legislação para incluir no tipo de tal artigo a expressão “dado eletrônico”.

Seguindo esse raciocínio, destaca-se que a edição das leis 12.735/12 e 12.737/12 foi o primeiro passo para a adequação do ordenamento jurídico brasileiro à ameaça dos crimes virtuais, à luz da Convenção de Budapeste.

5.2 DESNECESSIDADE DE TIPIFICAÇÃO DOS CRIMES VIRTUAIS

De modo diverso, a teoria oposta acredita que não existe necessidade de leis específicas para os crimes virtuais, afirmando que existem instrumentos jurídicos que dão conta de solucionar tais questões. Entre esses instrumentos destaca-se a interpretação analógica ou extensiva.

Faz-se necessário abordar a fundo a interpretação analógica a fim de diferenciá-la da analogia. Rogério Greco (2015, p. 90) ensina que o legislador penal, ao não poder prever todas as possíveis situações delituosas da vida em sociedade e que seriam similares àquelas já elencadas no Código Penal, permitiu a utilização da interpretação analógica, como um recurso para ampliar o alcance da norma penal. Continua o doutrinador ao afirmar que o Código Penal, inicialmente detalha todas as situações que se propôs a regular, de acordo com o princípio da legalidade. Posteriormente, porém, permite que tudo que for semelhante à tais situações também possa ser abrangido pelo mesmo dispositivo.

Dessa maneira, não deve existir dúvida quanto à possibilidade da admissão do uso da interpretação em relação à matéria penal. Passando à sua comparação com o recurso da analogia, ensina Fragoso:

> A analogia distingue-se da interpretação, porque constitui um processo de integração da ordem legal, e não meio de esclarecer o conteúdo da norma. Através da analogia aplica-se a lei a hipótese por ela não prevista, invocando-se substancialmente, o chamado argumento *a pari ratione*. Há aplicação analógica quando a norma se estende a caso não previsto, mas semelhante, em relação ao qual existem as mesmas razões que fundamentam a disposição legal. A analogia distingue-se da interpretação extensiva, porque nesta não falta a vontade da lei, mas tão-somente a expressão verbal que a ela corresponda. (FRAGOSO, 1985, p. 87, *apud* VIANNA, 2004).

A analogia preza por preencher possíveis lacunas existentes na lei com hipóteses semelhantes, aplicando-as no caso concreto. Enquanto isso, a interpretação tem por objetivo buscar o entendimento correto da *intentio legis*. Explica o autor Túlio Vianna Lima (2004): "Se na integração o intérprete acrescenta à norma elementos previamente não existentes, na interpretação extensiva, ele tão-somente revela a *intentio legis* já existente, porém não expressa verbalmente de forma adequada".

Tendo isso em vista, fica claro que a interpretação analógica pode ser utilizada na seara penal sem violar o princípio da legalidade. Em conformidade com esse entendimento, estabeleceu o Superior Tribunal de Justiça em sede de Recurso Especial:

> TRIBUTÁRIO. RECURSO ESPECIAL. ISS. LISTA DE SERVIÇOS. TAXATIVIDADE.INTERPRETAÇÃO EXTENSIVA. POSSIBILIDADE.
> 1. Embora taxativa, em sua enumeração, a lista de serviços admite interpretação extensiva, dentro de cada item, para permitir a incidência do ISS sobre serviços correlatos àqueles previstos expressamente. Precedentes do STF e desta Corte.
> 2. Esse entendimento não ofende a regra do art. 108, § 1º, do CTN, que veda o emprego da analogia para a cobrança de tributo não previsto em lei. Na hipótese, não se cuida de analogia, mas de recurso à interpretação extensiva, de resto

> autorizada pela própria norma de tributação, já que muitos dos itens da lista de serviços apresentam expressões do tipo "congêneres", "semelhantes", "qualquer natureza", "qualquer espécie", dentre outras tantas.
> **3. Não se pode confundir analogia com interpretação analógica ou extensiva. A analogia é técnica de integração, vale dizer, recurso de que se vale o operador do direito diante de uma lacuna no ordenamento jurídico. Já a interpretação, seja ela extensiva ou analógica, objetiva desvendar o sentido e o alcance da norma, para então definir-lhe, com certeza, a sua extensão. A norma existe, sendo o método interpretativo necessário, apenas, para precisar-lhe os contornos.**
> 4. Recurso especial improvido. (STJ - REsp: 121428 RJ 1997/0014040-7, Relator: Ministro CASTRO MEIRA, Data de julgamento: 01/06/2004. T2 - SEGUNDA TURMA, Data de Publicação: DJ 16/08/2004 p.156)

Utilizando-se desse entendimento jurisprudencial, mais uma vez demonstra Tangerino:

> Para esta corrente doutrinária, a utilização da interpretação analógica extensiva resolveria a questão da aplicabilidade das normas penais existentes para punir as novas condutas perpetradas por meio das novas tecnologias, abarcando, por exemplo, o "estelionato virtual", o "dano informático", o "furto eletrônico", os crimes contra a honra em meio *web*, a violação de correspondência (*email*) entre outras, aplicando-se, de forma extensiva a estas condutas, respectivamente, os tipos estampados no Código Penal nos artigos 171, 163, 155, 138, 139, 140 e 151. (TANGERINO, 2016).

Ambos os pensamentos expostos nessa seção, apesar de divergirem entre si, são dotados de argumentos sólidos que lhes sustentam no debate teórico. Contudo, o Direito não fica apenas no papel: é aplicado na vida cotidiana da sociedade. Por isso, torna-se essencial passar à análise de casos concretos da Justiça Penal brasileira para ver como são combatidos os crimes virtuais sobre outra perspectiva.

6 EXPOSIÇÃO JURISPRUDENCIAL PRÉVIA À LEI 12.737/2012

Como já dito anteriormente, os crimes virtuais em nossa nação já eram observados mesmo antes da legislação brasileira os preverem, através da "Lei Carolina Dieckmann". Apresenta-se, então, algumas jurisprudências que precedem a edição do referido dispositivo legal, primeiramente:

> PENAL. PROCESSO PENAL. CONFLITO DE JURISDIÇÃO. INQUÉRITO POLICIAL. FRAUDE BANCÁRIA. CAIXA ECONÔMICA FEDERAL. TRANSFERÊNCIA DE VALORES POR MEIO ELETRÔNICO (*INTERNET*). FURTO MEDIANTE FRAUDE. (ART. 155, § 4º, INC. II, CP). FORO DA CONSUMAÇÃO DO DELITO. LUGAR ONDE SITUADA A AGÊNCIA EM QUE MANTIDA A CONTA-CORRENTE LESADA. PRECEDENTES (STJ E TRF4).
> 1. Consolidou-se o entendimento de que a subtração de valores de conta-corrente ou conta-poupança - sem a autorização do titular e por meio de expediente eletrônico fraudulento (*Internet*) - configura o crime de furto mediante fraude (art. 155, § 4º, inc. II, CP).
> 2. Considerando que o delito de furto se consuma no momento em que a coisa móvel é retirada da esfera de disponibilidade da vítima e colocada em poder do agente, competente para apreciar o feito é o juízo do lugar onde situada a agência da CEF em que mantida a conta corrente lesada.
> 3. Precedentes do Superior Tribunal de Justiça e deste Tribunal (TRF-4 - CJ: 19995 SC 2009.04.00.019995-6, Relator: TADAAQUI HIROSE, Data de Julgamento: 15/10/2009, QUARTA SEÇÃO, Data de Publicação: D.E. 09/11/2009);

Outro julgado que corrobora com o entendimento da decisão jurisprudencial anterior é a decisão proferida pelo Tribunal de Justiça de São Paulo (TJ-SP), no ano de 2011, em sede de apelação:

> FURTO QUALIFICADO - AUTORIA DELITIVA PROVADA - RECURSO PROVIDO.
> Suficientes os elementos probatórios a demonstrar a autoria de agente que subtraiu coisa alheia móvel, mediante fraude realizada por meio da *internet*, de rigor o decreto condenatório. FURTO QUALIFICADO - REGIME CARCERÁRIO MAIS GRAVOSO - CONVENIÊNCIA DE REGIME INICIAL FECHADO. Pode o Juiz impor regime prisional inicialmente fechado, independente do montante da privativa de liberdade e a primariedade do réu, em observância com as circunstâncias presentes no fato delituoso, em conjunto com aquelas previstas no artigo 59, do Código Penal (TJ-SP - APL: 43972720068260541 SP 0004397-27.2006.8.26.0541, Relator: WILLIAN CAMPOS, Data de Julgamento: 01/03/2011, 4 Câmara de Direito Criminal, Data de Publicação: 02/03/2011);

Por fim, também importante a exposição de outro julgado, este proferido ainda no ano de 2006 pelo Tribunal Regional Federal da 1ª Região (TRF-1), que vêm, mais uma vez, a adotar o mesmo entendimento que os anteriores, em relação aos crimes virtuais:

> PENAL E PROCESSUAL PENAL. FRAUDE NA REDE MUNDIAL DE COMPUTADORES (*INTERNET*). ART. 171, § 3º, DO CP. COMPETÊNCIA DO LUGAR ONDE O AGENTE COMETE O DELITO.
> I - No caso concreto, não há que se falar no delito de furto, caracterizado pela subtração, mas sim em crime de estelionato qualificado (art. 171, § 3º, do CP), já que o fato investigado - utilização de meio fraudulento para sacar dinheiro de correntistas da Caixa Econômica Federal -, leva, em tese, à configuração deste último.
> II - Tratando-se de crime de estelionato, a competência para processá-lo e julgá-lo é do lugar em que o agente efetivamente obteve a vantagem indevida, ou seja, onde ocorreu o dano. Precedentes.
> III - Recurso desprovido. (TRF-1 - RCCR: 1640 GO 2006.35.03.001640-0, Relator: DESEMBARGADOR FEDERAL CÂNDIDO RIBEIRO, Data de Julgamento: 24/10/2006, TERCEIRA TURMA, Data de Publicação: 17/11/2006 DJ p.43).

Ao analisar tais decisões jurisprudenciais, assinala Camila Requião Fentanes da Silva (2013) ser evidente que através da interpretação analógica ou extensiva as condutas de subtração ou destruição de dados informáticos estão sim tutelados pelo Direito Penal pátrio, aplicando-se mesmo aos crimes cometidos via *internet*, a tipificação prevista nos artigos 155 e 163 do Código Penal. Continua dizendo que dessa forma, a edição de leis que versem especificamente sobre os crimes na *internet* não é necessária.

Tal ideia, exposta pela doutrinadora, é apoiada após o exame das decisões jurisprudenciais expostas anteriormente, já que não existe dúvidas quanto à utilização da interpretação, seja extensiva ou analógica, nelas. Mais do que isso, fica claro que o emprego de tais instrumentos do Direito Penal é feito de maneira extremamente satisfatória, permitindo ao magistrado o enfrentamento adequado da modalidade delitiva dos crimes virtuais fazendo o uso deles.

Uma das razões para o prevalecer deste entendimento é a grande morosidade observada no Poder Legislativo, relativa ao trâmite dos seus projetos de lei. Compartilhando desse sentimento, diz Vianna:

> Evidentemente que uma legislação penal moderna e bem elaborada que aborde todas as questões criadas pelos novos crimes por computador facilitaria, e muito, o trabalho dos operadores do Direito. O ideal, inclusive é que o tema fosse regulado por um tratado internacional aos moldes da Lei Uniforme de Genebra, já que a

> *Internet* é um fenômeno transnacional e, como tal, deveria ser regulamentada. No entanto, a lentidão com que se aprovam leis no Brasil é fato notório. Procuramos fugir do discurso simplista de que o Brasil precisa de uma lei que regulamente os crimes pela *Internet*. Preferimos o desafio da análise cuidadosa de nossa legislação penal, que, [...], já tipifica muitas das modernas condutas delituosas realizadas pela *Internet*. (VIANNA, 2000, p. 5)

Diante de tudo exposto, notamos que os magistrados há muito já enfrentavam os crimes virtuais, mesmo sem a existência de leis específicas sobre o assunto no Brasil, o que nos leva a corroborar com a última corrente, apresentada no tópico 5.2, de que não existe a necessidade de edição de leis especificas para tipificar tais condutas, já sendo o juiz munido de ferramentas satisfatórias para enfrenta-las.

7 CONCLUSÃO

Nos tempos atuais, a tecnologia está presente em praticamente todos os momentos do dia-a-dia do homem médio e da sociedade como um todo. O avanço tecnológico vivido atualmente engloba todas as esferas da vida coletiva, desse modo, levou à introdução do uso dos dispositivos tecnológicos hodiernos para fins lesivos à sociedade: os crimes virtuais ou cibernéticos, do inglês, *cybercrimes*. A sua existência fomentou diversos debates e discussões acerca de como devem tais crimes ser tratados no âmbito legal e qual é a melhor maneira para lhes enfrentarem, não existindo até hoje um consenso doutrinário que responda tais questionamentos.

No começo do trabalho foi notado que a sociedade encontra-se em constante evolução, e, consequentemente, os adventos tecnológicos, idem e, por esse motivo o Direito Penal deveria prezar por moldar-se às mudanças sociais e não ser deixado para trás. Porém, errada está a presunção que a única ferramenta existente no Direito Penal é a lei. O magistrado possui diversas cartas à manga para enfrentar a relativamente nova modalidade delituosa dos crimes virtuais, não sendo para isso necessária a edição de leis que tipifiquem toda e qualquer possível conduta criminosa que advenha de aparatos tecnológicos ou sejam feitas através da rede mundial de computadores. Até porque, nota-se que muitos dispositivos das leis já existentes acerca dos crimes cibernéticos no ordenamento jurídico brasileiro já vêm a vida eivados de imperfeições.

Isto não quer dizer que a lei 12.737/2012 foi totalmente inútil, longe disso. As suas alterações ao Código Penal pátrio foram pontuais em adicionar noções previamente impensadas no ordenamento jurídico brasileiro e munir os juízes penais de mais ferramentas para combater esses crimes cada vez mais comuns. Todavia, o entendimento defendido por alguns de que os crimes virtuais só poderão ser enfrentados caso exista tipificação específica para cada um significaria ignorar artifícios legais e de eficácia comprovada ao longo dos anos do Direito Penal brasileiro. Nesse sentido, é importante atentar-se para os precedentes jurisprudenciais no combate aos crimes cibernéticos, que mesmo antes da existência de qualquer lei específica que os tipificasse, mostram a possibilidade de enfrentamento satisfatório dessas condutas criminosas.

Importante notar que a edição de leis especificas poderia sim ser uma solução para o problema das condutas delituosas virtuais, sendo esse um pensamento defendido por Túlio Lima Vianna, um doutrinador de grande importância na discussão acerca das novas tecnologias e Direito Penal no âmbito nacional, porém, os problemas atrelados à tal, com destaque para a grande demora no trâmite dos projetos de lei no Poder Legislativo, tornam esta uma alternativa aquém do ideal, fato já previsto pelo autor tempos atrás, no ano de 2000.

Diante disso, conclui-se que a problemática da tipificação dos crimes virtuais no ordenamento jurídico brasileiro vai muito além da simples decisão por editar, ou não, leis que

tratem do assunto. Trata-se também da conjuntura política do Brasil atual e da inegável morosidade do Poder Legislativo. Prova disso é a publicação da lei 12.735/2012 ou "Lei Azeredo", que só veio a acontecer mais de uma década após o projeto de lei que lhe idealizou e como notado, só se efetivou devido ao apelo popular e midiático decorrente de um caso que ganhou notoriedade no país ao envolver uma celebridade. Dessa maneira, defende-se a falta de necessidade de edição de legislação especializada para os crimes cibernéticos, tendo em vista a perfeita aplicação da interpretação analógica aos casos concretos.

REFERÊNCIAS

BARBOSA JUNIOR, Sergio Jose. **Crimes informáticos: breves considerações sobre os delitos virtuais no ordenamento jurídico brasileiro**. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 19, n. 4008, 22 jun. 2014. Disponível em: <https://jus.com.br/artigos/29634>. Acesso em: 22 out. 2019.

BRASIL. Constituição (1988). **Constituição: República Federativa do Brasil**. Brasília: Centro gráfico, 2018.

BRASIL. **Decreto-Lei nº 3.914, de 09 de dezembro de 1941**. Lei de introdução do Código Penal (decreto-lei n. 2.848, de 7-12-940) e da Lei das Contravenções Penais (decreto-lei n. 3.688, de 3 outubro de 1941). Brasília, DF, 9 dez. 1941. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del3914.htm>. Acesso em: 25 out. 2019.

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. Brasília, DF, 30 nov. 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 20 out. 2019.

BRASIL. **Lei nº 12.735, de 30 de novembro de 2012**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Brasília, DF, 30 nov. 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm>. Acesso em: 23 out. 2019.

BRASIL. Superior Tribunal de Justiça. **RECURSO ESPECIAL: REsp 121428 RJ 1997/0014040-7**. Relator: Ministro Castro Meira. DJ: 01/06/2004. In: JusBrasil, 2004. Disponível em: <https://stj.jusbrasil.com.br/jurisprudencia/19466897/recurso-especial-resp-121428-rj-1997-0014040-7?ref=juris-tabs>. Acesso em: 27 out. 2019.

BRASIL. Tribunal Regional Federal. **CONFLITO DE JURISDIÇÃO: CJ 19995 SC 2009.04.00.019995-6**. Relator: Tadaaqui Hirose. DJ: 15/10/2009. In: JusBrasil, 2009. Disponível em: <https://trf-4.jusbrasil.com.br/jurisprudencia/6925575/conflito-de-jurisdicao-cj-19995-sc-20090400019995-6-trf4>. Acesso em: 09 nov. 2019.

BRASIL. Tribunal de Justiça de São Paulo. **APELAÇÃO: APL 0004397-27.2006.8.26.0541 SP 0004397-27.2006.8.26.0541**. Relator: Willian Campos. DJ: 01/03/2011. In: JusBrasil,

2009. Disponível em: <https://tj-sp.jusbrasil.com.br/jurisprudencia/18384911/apelacao-apl-43972720068260541-sp-0004397-2720068260541>. Acesso em: 09 nov. 2019.

BRASIL. Tribunal Regional Federal. **RECURSO CRIMINAL: RCCR 1640 GO 2006.35.03.001640-0.** Relator: Desembargador Federal Cândido Ribeiro. DJ: 24/10/2006. In: JusBrasil, 2009. Disponível em: <https://trf-1.jusbrasil.com.br/jurisprudencia/2218921/recurso-criminal-rccr-1640-go-20063503001640-0>. Acesso em: 09 nov. 2019.

CARNEIRO. Adeneele Garcia. **Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação**. In: Âmbito Jurídico, 2012. Disponível em: <https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-uma-reflexao-sobre-o-problema-na-tipificacao/>. Acesso em: 02 nov. 2019.

COSTA, Marco Aurélio Rodrigues da. **Crimes de Informática**. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 2, n. 12, 5 maio 1997. Disponível em: https://jus.com.br/artigos/1826. Acesso em: 8 nov. 2019.

DA SILVA, Camila Requião Fentanes. **Análise das Leis nº 12.735/2012 e 12.737/2012 e a (des)necessidade de uma legislação específica sobre crimes cibernéticos**. In: JusBrasil, 2014. Disponível em: <https://jus.com.br/artigos/32265/analise-das-leis-n-12-735-2012-e-12-737-2012-e-a-des-necessidade-de-uma-legislacao-especifica-sobre-crimes-ciberneticos/1>. Acesso em: 23 out. 2019.

FRUHLINGER,Josh. **What is phishing? How this cyber attack works and how to prevent it**. In: CSO, 2019. Disponível em: <https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html>. Acesso em: 27 out. 2019.

FURLANETO NETO, Mário e GUIMARÃES, José Augusto Chaves. **Crimes na *internet*: elementos para uma reflexão sobre a ética informacional**. Brasília, 2003. Disponível em: <http://www.egov.ufsc.br/portal/conteudo/crimes-na-*HYPERLINK "http://www.egov.ufsc.br/portal/conteudo/crimes-na-internet-elementos-para-uma-reflex%C3%A3o-sobre-%C3%A9tica-informacional"internet*HYPERLINK "http://www.egov.ufsc.br/portal/conteudo/crimes-na-internet-elementos-para-uma-reflex%C3%A3o-sobre-%C3%A9tica-informacional"-elementos-para-uma-reflex%C3%A3o-sobre-%C3%A9tica-informacional> Acesso em: 20 out. 2019.

GELBERT, Laura. **Brasil está entre os cinco países com mais crimes cibernéticos, aponta relatório da ONU**. Nova York, 2015. Disponível em: http://www.ebc.com.br/tecnologia/2015/03/brasil-esta-entre-os-cinco-paises-com-mais-crimes-ciberneticos-aponta-relatorio. Acesso em: 18 out. 2019.

GRECO, Rogério. **Curso de Direito Penal: Parte Geral**. 17 ed., rev., ampl. e atual., Rio de Janeiro: Impetus, 2015.

KLEINA, Nilton. **A história da *Internet*: pré-década de 60 até anos 80**. In: Tecmundo, 2011. Disponível em: <https://www.tecmundo.com.br/infografico/9847-a-historia-da-internet-pre-decada-de-60-ate-anos-80-infografico-.htm>. Acesso em: 21 out. 2019.

LIMA. Simão Prado. **Crimes virtuais: uma análise da eficácia da legislação brasileira e o desafio do direito penal na atualidade**. In: Âmbito Jurídico, 2014. Disponível em: <https://ambitojuridico.com.br/cadernos/direito-penal/crimes-virtuais-uma-analise-da-eficacia-da-legislacao-brasileira-e-o-desafio-do-direito-penal-na-atualidade/>. Acesso em: 01 nov. 2019.

LOVELUCK, Benjamin. **Redes, liberdades e controle: Uma genealogia política da *internet***. 1 ed., Rio de Janeiro: Vozes, 2018.

MENDES, Priscilla. Dieckmann foi chantageada em R$ 10 mil por fotos, diz advogado. **G1**. Brasília, 05 de maio de 2012. Disponível em: <http://g1.globo.com/tecnologia/noticia/2012/05/dieckmann-foi-chantageada-em-r10-mil-devido-fotos-diz-advogado.html>. Acesso em 23 out. 2019

NETO, Guilherme. **Top 10: principais ataques de *phishing* da Internet**. 2012. Disponível em: <https://www.techtudo.com.br/noticias/noticia/2012/02/top-10-principais-ataques-de-phishing-da-internet.html> Acesso em: 28 out. 2019

NUCCI, Guilherme de Souza. **Manual de direito penal**. 11 ed., rev., ampl. e atual., Rio de Janeiro: Forense, 2015.

PETER, Ian. ***Ian Peter's History of the Internet: The beginnings of the Internet***. In: NetHistory, 2003. Disponível em: <http://www.nethistory.info/History%20of%20the%20Internet/beginnings.html>. Acesso em: 05 out. 2019.

PINHEIRO, Reginaldo César. ***Os cybercrimes na esfera jurídica brasileira***. Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 5, n. 44, 1 ago. 2000. Disponível em: https://jus.com.br/artigos/1830. Acesso em: 8 nov. 2019.

SILVEIRA, Neil; SOUSA, Mirian Lima de; MELO, Antonia Morgana Alcantara Jorge. **Crimes cibernéticos e invasão de privacidade à luz da lei Carolina Dieckmann**. Revista Jus Navigandi, 2017. Disponível em: <https://jus.com.br/artigos/61325/crimes-ciberneticos-e-invasao-de-privacidade-a-luz-da-lei-carolina-dieckmann/1>. Acesso em: 26 out. 2019.

SOUZA, Gills Lopes Macêdo e PEREIRA, Dalliana Vilar. **A Convenção de Budapeste e as leis brasileiras**. Disponível em: <http://www.academia.edu/786458/A_CONVENCAO_DE_BUDAPESTE_E_AS_LEIS_BRASILEIRAS> Acesso em: 27 out. 2019.

TANGERINO. Dayane Fanti. **Direito penal e novas tecnologias**. Porto Alegre, 2016. Disponível em: <https://canalcienciascriminais.com.br/direito-penal-e-novas-tecnologias/>. Acesso em: 23 out. 2019.

VIANNA, Túlio Lima. **3 críticas ao Projeto de Lei de Crimes Informáticos**. Rio de Janeiro, 2009. Disponível em: <https://politics.org.br/edicoes/3-cr%C3%ADticas-ao-projeto-de-lei-de-crimes-inform%C3%A1ticos>. Acesso em: 01 nov. 2019.

VIANNA, Túlio Lima. Do delito de dano e de sua aplicação ao Direito Penal informático. **Revista Jus Navigandi**, ISSN 1518-4862, Teresina, ano 9, n. 482, 1 nov. 2004. Disponível em: https://jus.com.br/artigos/5828. Acesso em: 02 nov. 2019.

VIANNA, Tulio Lima. **Dos crimes pela *internet***. Belo Horizonte, 2000, p. 5. Disponível em: <https://www.academia.edu/1911162/Dos_crimes_pela_internet> Acesso em: 01 nov. 2019

VIANNA, Túlio Lima. **Fundamentos de direito penal informático: do acesso não autorizado a sistemas computacionais**. 1ª ed., Rio de Janeiro: Forense, 2003.