FACULDADE VIASAPIENS – FVS
CURSO DE GRADUAÇÃO EM DIREITO

CARLA EVELYN SILVA SOUZA

CIBERCRIMINALIDADE: ANÁLISE DA EVOLUÇÃO DA LEGISLAÇÃO BRASILEIRA SOBRE CRIMES VIRTUAIS

Tianguá – CE
2023.2

CARLA EVELYN SILVA SOUZA

CIBERCRIMINALIDADE: ANÁLISE DA EVOLUÇÃO DA LEGISLAÇÃO BRASILEIRA SOBRE CRIMES VIRTUAIS

Monografia apresentada a Faculdade ViaSapiens – FVS como requisito parcial para a obtenção do título de Bacharel em Direito.

Orientador(a): Professor Esp. Tiago Oliveira Freire Carneiro

Orientador metodológico: Professor Esp. Francisco Danilo de Souza Gomes.

Tianguá – CE

2023.2

Dados Internacionais de Catalogação na Publicação
Ficha catalográfica elaborada pela Biblioteca da Faculdade ViaSapiens
com os dados fornecidos pelo(a) autor(a)

S586c

Silva Souza, Carla Evelyn.
Cibercriminalidade: Análise da evolução da legislação brasileira sobre crimes virtuais / Carla Evelyn Silva Souza - 2023.
48 f.

Trabalho de Conclusão de Curso (graduação) - Faculdade ViaSapiens, Bacharelado em Direito. Tianguá. 2023

Orientação: Esp. Tiago Oliveira Freire Carneiro
Coorientação: Esp. Francisco Danilo de Souza Gomes
1. Crimes cibernéticos. 2. Internet. 3. Legislação.

CDD 003.5

FACULDADE VIASAPIENS – FVS
ATA DE DEFESA DE MONOGRAFIA DO CURSO DE DIREITO

Em 25 de novembro de 2023, às 09:30 h, no Auditório 02 da Faculdade ViaSapiens, de modo presencial, compareceram para a **DEFESA PÚBLICA DE MONOGRAFIA** do curso de graduação Direito, requisito obrigatório para a obtenção da aprovação na disciplina de Trabalho de Conclusão de Curso II, o(a) aluno(a): **CARLA EVELYN SILVA SOUZA,** tendo como título do Trabalho **CIBERCRIMINALIDADE: ANÁLISE DA EVOLUÇÃO DA LEGISLAÇÃO BRASILEIRA SOBRE CRIMES VIRTUAIS**, e os professores que constituíram a Banca Examinadora:

a) Professor(a)-orientador(a): Prof. Esp. Tiago Oliveira Freire Carneiro
b) Professor(a)-examinador(a): Profa. Esp. Francisco Maxvânio Parente Vasconcelos;
c) Professor(a)-examinador(a): Profa. Esp. Francisco Danilo de Souza Gomes;

Após a apresentação da Monografia e as observações dos membros da banca avaliadora, ficou definido que o trabalho foi APROVADO, com média 10, (DEZ), a partir das seguintes notas:

EXAMINADOR(A)	NOTA	VISTO
Prof. Esp. Tiago Oliveira Freire Carneiro	10	
Profa. Esp. Francisco Maxvânio Parente Vasconcelos;	10	
Profa. Esp. Francisco Danilo de Souza Gomes;	10	

Eu, **Tiago Oliveira Freire Carneiro**, professor(a)-orientador(a), lavrei a presente ata, que segue assinada por mim e pelos demais membros da Banca Examinadora.

Reformulações:
( ) Não.
( ) Sugeridas
( ) Exigidas

Professor(a) Esp. Tiago Oliveira Freire Carneiro
Orientador(a)

Professor(a) Esp. Francisco Maxvânio Parente Vasconcelos
Examinador(a)

Professor(a) Esp. Francisco Danilo de Souza Gomes
Examinador(a)

Carla Evelyn Silva Souza
CARLA EVELYN SILVA SOUZA – ALUNO (A)

Dedico esse estudo monográfico aos meus pais, meus pilares e maiores incentivadores para à realizações dos meus sonhos.

AGRADECIMENTOS

Em primeiro lugar agradeço a Deus, pois sem sua graça não seria capaz de chegar até aqui. Aos meus pais, agradeço por todo suporte durante toda minha trajetória, me auxiliando e encorajando, sendo sempre minhas maiores fontes de inspiração.

À minha tia e segunda mãe, Zélia, que sempre estiveram ao meu lado me apoiando ao longo da vida. À minha irmã, Andressa, por ser minha maior companhia, sei que independente do momento, sempre estará ao meu lado. Ao Jerfessom por sempre está ao meu lado, me apoiando e incentivando durante esses 5 anos de graduação. Às minhas amigas, em especial, Milena e Vanessa, agradeço pelo carinho, por fazerem momentos de puro estresse se tornarem mais leves e por estarem tão presentes em minha vida, mesmo com a distância e nossos encontros não sejam mais tão frequentes.

Agradeço aos meus colegas de sala, Vera, Renata, Tácila e Roberto pela espontaneidade e alegria na troca de conhecimentos, ao qual guardarei para sempre em meu coração. Aos professores da graduação por terem contribuído para o meu aprendizado durante esses anos.

Agradeço ao professor Tiago Oliveira, por ter aceitado ser meu orientador e por todo apoio e orientação.

Por fim, expresso minha gratidão a todos aqueles que, de alguma maneira, contribuíram para minha trajetória e desenvolvimento acadêmico.

“Sonhos determinam o que você quer. Ações determina o que você conquista.”

- Aldo Novak

RESUMO

As tecnologias evoluem de modo acelerado em torno do mundo, com a expansão da internet, e as facilidades oferecidas pelo ambiente virtual, especialmente elementos como a ilusão de anonimato e a conveniência, têm exercido uma influência significativa no aumento dos crimes no ciberespaço. Neste trabalho, durante os capítulos serão analisados os avanços legislativos brasileiros referentes aos crimes virtuais, apurando-se as principais críticas direcionadas a essas normas, abordados desde os aspectos históricos da tecnologia, bem como os marcos evolutivos e conceituais dos crimes cibernéticos, trazendo suas classificações e principais espécies. Após a construção de três capítulos é possível concluir que ainda há necessidade de maior eficácia, adequação quando a aplicabilidade dos mecanismos legais e o preenchimento de lacunas normativas.

Palavras-chave: Crimes cibernéticos. Internet. Legislação.

ABSTRACT

Technologies evolve rapidly around the world, with the expansion of the internet, and the facilities offered by the virtual environment, especially elements such as the illusion of anonymity and convenience, have had a significant influence on the increase in crimes in cyberspace. In this work, during the chapters, Brazilian legislative advances regarding virtual crimes will be analyzed, investigating the main criticisms directed towards these norms, covered from the historical aspects of technology, as well as the evolutionary and conceptual milestones of cyber crimes, bringing their classifications. and main species. After constructing three chapters, it is possible to conclude that there is still a need for greater effectiveness, adaptation to the applicability of legal mechanisms and the filling of regulatory gaps.

Keywords: Cyber Crimes. Internet. Legislation.

LISTA DE SIGLAS

ENIAC – Computador integrador numérico eletrônico.

ARPANET – Agência de pesquisa em projetos avançados.

RNP – Rede Nascional de Pesquisa.

CGI – Comitê gestor da internet.

FAPESP – Fundação de Amparo à Pesquisa do Estado de São Paulo.

LNCC – Laboratório Nacional de Computação Científica.

RNP – Rede Nacional de Pesquisas.

IBGE – Instituto Brasileiro de Geografia e Estatística.

WWW – World Wide Web

LISTA DE ILUSTRAÇÕES

SUMÁRIO

INTRODUÇÃO

Com o crescimento da utilização da internet ao longo dos anos, concomitantemente com a quantidade de usuários, que buscam recursos que viabilizam a facilitação de alguma área de suas vidas, sejam em busca de informações, entretenimento, relações comerciais, a rápida ascensão da tecnologia e a conexão global proporcionada pela internet, houve inúmeros benefícios, entretanto, introduziu consigo novos desafios sociais, pois também proporciona uma crescente exposição desses usuários, facilitando cada vez mais a utilização de meios virtuais para à prática de delitos.

Os cibercrimes podem ocorrer de várias formas, em qualquer horário ou lugar, sendo usados diferentes métodos em acordo com seus objetivos, tendo como seu maior aliado do autor a facilidade de se esconder atrás dos meios eletrônicos, não tendo necessidade de estar próximo ou nem mesmo de conhecer a vítima, podendo o autor do delito está em qualquer lugar do mundo, em conjunto com a falta de regulamentação e fiscalização adequadas, trata-se de um problema cada vez mais comum, onde muitas pessoas ainda não estão cientes dos riscos e ameaças que enfrentam online.

Embora grande parte dos crimes cometidos em ambientes digitais estejam relacionados com crimes já tipificados pelo código penal brasileiro de 1940, com o passar dos anos, mostrou-se indispensável que a legislação busque adequar-se à nova realidade, e o por essa razão trabalho busca a realizar uma análise da evolução da legislação brasileira no que tange aos crimes cibernéticos.

A cibercriminalidade, caracterizada por atividades ilícitas que exploram as fraquezas do mundo digital, ultrapassando fronteiras geográficas e desafiando as formas tradicionais de combater o crime, por serem crimes que geralmente não ameaçam diretamente a vítima da mesma forma que os crimes tradicionais, a legislação para prevenir esses delitos precisa ser diferente. Isso significa que as leis devem ser descritas e ajustadas para punir os responsáveis e garantir a segurança da população. Uma dificuldade adicional é a rapidez com que a tecnologia avança em comparação com o desenvolvimento das leis.

A metodologia utilizada para pesquisa deste trabalho foi bibliográfica, respaldada pela legislação, doutrinas e artigos científicos sobre o tema. Perante a

problemática, busca verificar como legislação brasileira tem respondido ao longo dos anos as práticas delituosas diante as rápidas mudanças no cenário tecnológico.

Serão abordadas durante o primeiro capítulo, noções gerais sobre a evolução tecnológicas, tratando-se do conceito e de como a internet surgiu desde seu uso restrito até seu período de expansão para o uso comercial, será visto também o conceito de cibercriminalidade, sua origem, primeiros casos e classificações.

No segundo capítulo serão expostas as principais espécies de crimes virtuais que ocorrem atualmente, sendo elas o crime contra a honra, crimes de invasão de privacidade e intimidade, estelionato virtual, crimes contra a liberdade sexual de menores e a violência virtual contra a mulher.

Por fim será abordado como a legislação nacional tem respondido aos desafios impostos pelo cenário de delitos cibernético ao longo dos anos.

Dessa forma, a presente monografia tem como objetivo apresentar quais os crimes praticados nos ambientes virtuais e analisar os resultados dessas condutas delituosas no direito brasileiro.

1. ASPECTOS EVOLUTIVOS E CONCEITUAIS DA TECNOLOGIA E DA CRIMINALIDADE CIBERNÉTICA

Inicialmente, para que se possa falar sobre a criminalidade virtual é necessário compreender como se deu o processo de evolução que levou o mundo a tal problemática, como o fenômeno da globalização transformou o modo de vida de todo o globo, onde diante das grandes evoluções da era atual, assim como há mudanças nos meios tecnológicos, a sociedade vem sendo transformada diariamente por influência das tecnologias, e trazendo novas formas de relações entre as pessoas e os equipamentos eletrônicos, fez com que a internet e os dispositivos eletrônicos se tornaram parte integrante da vida em sociedade.

Essa nova realidade social trouxe notáveis avanços e comodidades, onde acesso a meios digitais pelos cidadãos, que buscam se adaptar a era virtual, se torna cada vez mais fácil, já que grande parte da população possui acesso à Internet, por intermédio de computadores, smartphones e outros dispositivos eletrônicos, para os quais as formas de se adquirir e de se utilizar são gradativamente mais simplificadas, trazendo a todos a oportunidade de romper barreiras de comunicação com o mundo, mediante um processo simples, usual e dinâmico, trazendo benefícios, mas, ao mesmo tempo, consequências negativas, por também se tornar um meio para prática de atividade ilícitas.

1.1. NOÇÕES GERAIS SOBRE A EVOLUÇÃO TECNOLÓGICA

De acordo com Walter Isaacson (2014), a Segunda Guerra Mundial, foi a responsável por mostrar ao mundo a necessidade de impulsionar os avanços tecnológicos, visto que na época, quase todas as grandes conquistas tecnológicas eram resultados apenas de atividades militares, essa necessidade foi fomentada com a entrada dos Estados Unidos na guerra, em dezembro de 1941, dando assim o impulso necessário para fornecer apoio financeiro o projeto dos engenheiros e cientistas americanos, John W.Mauchly e J.Presper Eckert, em 9 de abril de 1943.

Assim, em 1946, foi anunciado a criação do ENIAC, Electrical Numerical Integrator and Calculator, computador integrador numérico eletrônico, o primeiro computador eletrônico e digital do mundo, que teve sua construção iniciada em junho de 1943, pesando cerca de 300 (trezentas) toneladas e ocupando uma área

de 270m², foi projetado em regra para resolver cálculos balísticos, cálculos que antes eram feitos por um analisador, que havia sido inventado pelo instituto de tecnologia de Masschusetts que para apenas um tipo de projétil era necessário calcular cerca de 3 mil trajetos, em conjunto com os cálculos feitos pela máquina eram também necessários o trabalho de 170 pessoas, que em maioria eram mulheres, e mesmo com todo esse esforço era preciso mais de mês para que uma tabela de disparos fosse completa, com toda essa demora, era evidente que esse trabalho não era mais suficiente, pois uma parte da artilharia norte-americana ficava ineficaz (Isaacson, 2014).

Já a internet, teve sua história iniciada no ambiente da Guerra Fria, em 1958, com a criação da Advanced Research Projects Agency (ARPA), tendo como principal objetivo acelerar o desenvolvimento tecnológico do país, mobilizando recursos de pesquisas universitárias para alcançar uma superioridade tecnológica militar em relação à União Soviética (Castells, 2003).

Foi por meio da Arpanet, como era chamada a internet, que se teve a primeira conexão estabelecida, em 1969, por meio de uma troca de e-mail entre a universidade da Califórnia e o Instituto de Pesquisa de Stanford, que buscava garantir que ocorria comunicação entre militares e cientistas de forma segura. Por duas décadas a internet era usada apenas no âmbito acadêmico, sendo liberado para o uso comercial apenas em 1987, nos Estados Unidos, e assim surgindo até 1992, quando surgiu os primeiros provedores de acesso à internet (Silva, 2001).

Segundo Manuel Castells (2003):

> A história da criação e do desenvolvimento da Internet é a história de uma aventura humana extraordinária. Ela põe em relevo a capacidade que tem as pessoas de transcender metas institucionais, superar barreiras burocráticas e subverter valores estabelecidos no processo de inaugurar um mundo novo. Reforça também a ideia de que no processo de que a cooperação e a liberdade de informação podem ser mais propícias à inovação do que a competição e os direitos de propriedade.

A ARPANET foi o marco inicial no desenvolvimento da internet, entretanto, foram as várias implementações ao longo dos anos que a aprimoraram até chegar à forma em que é conhecida atualmente.

Conforme Castells (2003), a concepção da internet tal como a conhecida hoje teve origem em 1994 com a introdução da World Wide Web (WWW), a "WEB". Essa inovação foi desenvolvida por Tim Berners-Lee, um inglês, enquanto

trabalhava no Centro Europeu de Investigação Nuclear (CERN) em Genebra, foi através da WEB, que começou a possibilidade de envio de imagens, vídeos e sons, anteriormente só era possível a transmissão de textos.

Vilha (2002) descreve a internet como um conjunto de ferramentas que permite explorar a World Wide Web através de textos interativos com links em forma de palavras, títulos, imagens ou fotografias, conectando páginas dentro do mesmo computador ou entre computadores distintos onde A World Wide Web é a área que experimenta o maior crescimento na internet, ocupando cada vez mais os espaços que antes eram ocupados por interfaces mais antigas da rede.

No Brasil, o primeira conexão de Internet foi realizado, em 1988, por iniciativa da Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), por uma parceria com o Fermi National Accelerator Laboratory (FERMILAB), sendo reconhecido como um dos mais importantes centros de investigação nos Estados Unidos. Universidade Federal do Rio de Janeiro (UFRJ) e o Laboratório Nacional de Computação Científica (LNCC) seguiram a mesma ideia, e também obtiveram uma conexão no mesmo período. E em 1992, com a criação da Rede Nacional de Pesquisas (RNP), pelo governo federal brasileiro, se desenvolveu uma extensa infraestrutura para sustentar a expansão da internet global, onde recebia dados internacionais e os disseminavam pelas principais cidades do país. Já no ano de 1996, foi criado o CGI, o comitê gestor da internet, formado por universidades, provedores de rede, ONGs e pelos principais órgãos do governo (Vieira, 2003).

A lei 12.965 de 2014 considera a internet como:

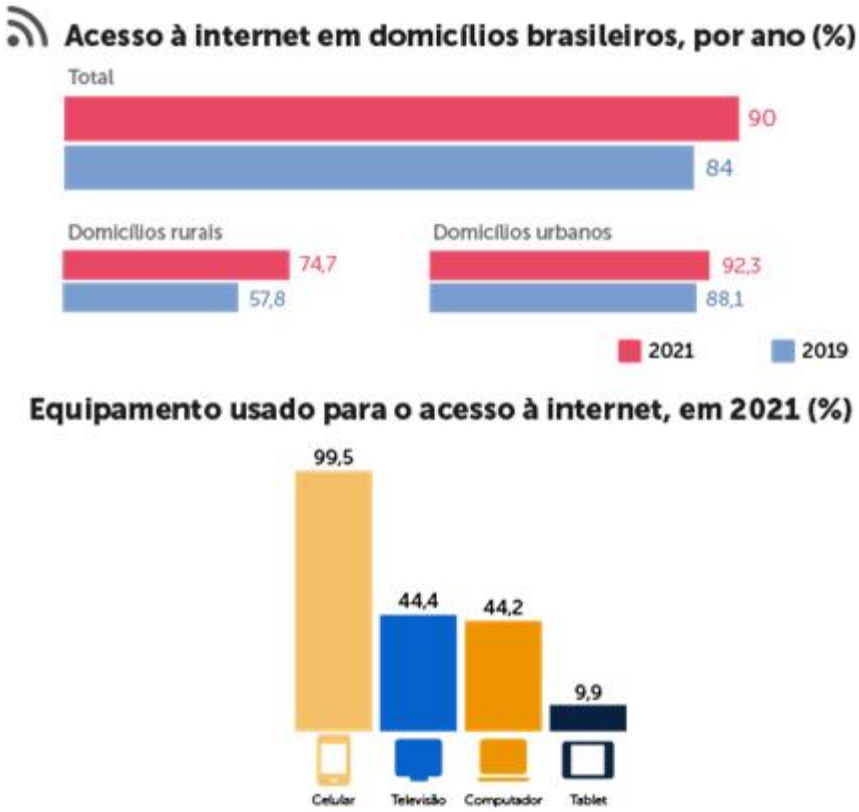
> O sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes (Brasil, 2014).

A internet no Brasil, por um período, era apenas explorado no ramo acadêmico, tendo sua a exploração comercial no país iniciado apenas no fim de 1994, através de um projeto da Embratel, que permitiu conexão por linhas discadas, em caráter experimental, onde cinco mil usuários tiveram a oportunidade de testar o serviço, e apenas no ano seguinte o acesso à internet via Embratel passou a funcionar definitivamente, com o objetivo da não monopolização do acesso à internet no Brasil surgiu o comitê gestor de internet, buscando estabelecer os rumos de

implementação administração e uso do acesso à internet no país, coletando, organizando e disseminando informações sobre os serviços da internet.

E desde então o uso dessas tecnologias vem se expandindo progressivamente com o passar dos anos, ganhando a cada dia uma nova finalidade, no Brasil, conforme o IBGE (Instituto Brasileiro de Geografia e Estatística), em 2021 a Internet foi utilizada em 90% dos domicílios do país, e o número de domicílios com celulares era de 96,3%.

Figura 1: Pesquisa Nacional por Amostra de Domicílios Contínua



Fonte: IBGE (2021)

Essas transformações intrínsecas do universo tecnológico e digital surgiram com o intuito de tornar a vida das pessoas mais simples, graças à sua capacidade de adaptação, flexibilidade e praticidade, no qual os computadores e a internet, que antes tinham um uso restrito e um deslocamento quase impossível, passaram de armas de força militar para um produto de comércio lucrativo, possível para a grande parte da população mundial, aonde partir dos anos 2000, com o surgimento das redes sociais e a facilitação de acesso ao universo online, tais tecnologias acabaram por transformarem-se em uma força motriz que molda a forma

como as pessoas vivem, trabalham, se relacionam, comunicam e compartilham informações.

1.2 NOÇÕES HISTÓRICAS E CONCEITUAIS SOBRE A CIBERCRIMINALIDADE

Diante as inúmeras vantagens trazidas pela internet, é necessário também se observar todos os riscos que ela traz, e por essa razão, onde sociedade vem sendo transformada diariamente por influência das tecnologias, o Direito percebeu a necessidade de se moldar a esta nova realidade, pois é inevitável dizer que a Internet se tornou um recurso indispensável no dia a dia das pessoas, que vem aumentando gradualmente devido às facilidades com computadores, smartphones e demais dispositivos. Diante de toda essa disseminação e facilitação eletrônicas, a internet foi vista como um meio simples de criminosos alcançarem um vasto número de vítimas, assim surgindo a cibercriminalidade.

Existem diversas nomenclaturas utilizadas para descrever uma inflação criminal realizada por meio de um dispositivo eletrônico ou por uma rede conectada à internet. Algumas delas incluem: crimes virtuais, delitos online, cibercrimes, crimes digitais, entre outras. De uma forma ou de outro, todas as nomenclaturas se referem a mesma conduta. O termo cibercrime teve sua origem em Lyon, na França, no fim da década de 1990, em uma reunião de um subgrupo das nações G-8.

A designação utilizada para indicar a origem das ações criminosas na internet recebe diversas denominações, como Mundo Virtual, Ciberespaço, Espaço Cibernético, Cyberspace, essa terminologia não segue uma uniformidade mundial, variando conforme o país e sua respectiva legislação. Foi na década de 1960 que surgiram os primeiros infratores que exploravam as tecnologias associadas a computadores e à internet. Eles faziam uso de seus conhecimentos para obter acesso a informações confidenciais de usuários e de empresas de grande relevância, incluindo multinacionais e empresas de diversos setores (Souza; Volpe, 2015).

Para Pinheiro (2021) crimes virtuais são:

> Podemos conceituar os crimes virtuais como sendo as condutas de acesso não autorizado a sistemas informáticos, ações destrutivas nesses sistemas, a interceptação de comunicações, modificações de dados, infrações os direitos de autor, incitação ao ódio e descriminação, chacota religiosa, transmissão de pornografia infantil, terrorismo, entre diversas outras formas existente.

Rossini (2004), aduz que os delitos informáticos, pode ser definido como uma conduta típica e ilícita, caracterizada como crime ou contravenção, cometida de forma dolosa ou culposa, por pessoa física ou jurídica. Essa conduta pode ser tanto comissiva quanto omissiva, ocorrendo tanto em ambientes de rede quanto fora deles. O ponto central desse delito está relacionado ao uso da informática e à violação direta ou indireta da segurança informática, que abrange os elementos de integridade, disponibilidade e confidencialidade.

Devido ao avanço constante da tecnologia, a luta contra os delitos cibernéticos torna-se cada vez mais desafiadora. Com o uso da internet, indivíduos com conhecimentos avançados têm passado a obtenção de forma indevida informações criptografadas, muitas vezes visando obter ganhos financeiros ou simplesmente por diversão (Jesus; Milagres, 2016).

Como explicam Damásio de Jesus e José Milagres (2016), ainda há uma divergência doutrinaria sobre qual seria o primeiro registro de crime cibernético registrado no mundo, pois algumas doutrinas o primeiro teria ocorrido no Instituto de tecnologia de Massachusetts, MIT, em 1964, onde um aluno de 18 anos teria cometido um delito que poderia ser classificado com cibercrime, onde advertido pelos superiores. Outra parte da doutrina acredita que o primeiro caso de que se tem notícia sobre hacking, em 1978, ocorreu na Universidade de Oxford, onde um estudante invadiu uma rede de computadores e copiou uma prova. Nessa época ainda não existia lei sobre crimes cibernéticos nos Estados Unidos, mas foi nesse mesmo ano, no estado da Flórida, foi formulado a primeira lei sobre o assunto nos Estados Unidos.

Também foi na década de 1970, que surgiu o termo norte-americano Hacker, designação foi utilizada para categorizar indivíduos que identificavam falhas no sistema de rede da internet por meio de computadores. Outra denominação amplamente difundida foi o termo "Cracker", que não apenas possuía um conhecimento mais aprofundado sobre as vulnerabilidades dos computadores, mas também se envolvia em atividades de roubo e exclusão de informações cruciais pertencentes a outros usuários na rede (Souza; Volpe, 2015).

A ascensão da internet e sua arquitetura que permite a interconexão de dispositivos sem restrições geográficas ou controle, juntamente com a facilidade de troca de informações entre usuários que podem nunca se encontrar pessoalmente, criou um ambiente propício para o surgimento de uma nova categoria de programas

com o propósito de causar danos a terceiros. Um exemplo desses programas é o conhecido vírus de computador. Em termos simples, os vírus são programas de computador desenvolvidos com intenções maliciosas, geralmente destinados a causar danos a um grupo específico de computadores ou à rede como um todo. (Moreira, 2004).

Foi no ano de 1988, que o primeiro hacker foi condenado pela nova Lei de Fraude e Abuso de computador, norte-americana, Robert Morris foi o criador do primeiro vírus de computador do mundo, que infectou 6 mil computadores. Já no Brasil a primeira notícia de phishing scam bancário, foi em 1997. Outro caso igualmente importante no país foi em 1999, onde um empresário e ex-controlador de uma rede de varejo, foi acusado de enviar, de Londres, e-mails com informações falsas sobre o risco de quebra de um banco para o mercado financeiro. Mas foi em 2002 que o Brasil teria o título de maior “exportador” de crimes pela internet e em 2004 a primeira condenação por pirataria no país, um jovem de apenas 19 anos, condenado a seis anos e 4 meses por golpes no Brasil e nos Estados Unidos, entretanto tal condenação não veio de uma norma que regulasse diretamente crimes informáticos, mas sim embasada no que o Código Penal brasileiro fala sobre violação de direitos autorais (Jesus; Milagre, 2016).

A primeira iniciativa internacional voltada para abordar o tema de cibercrime foi a Conferência sobre Aspectos Criminológicos do Crime Econômico, que ocorreu no âmbito do Conselho da Europa, em 1976, em Estrasburgo. Entretanto, foi entre as décadas de 1980 e 1990 que grande parte dos cibercrimes se propagou.

A partir desse ponto, houve intensos debates sobre os desafios ligados à investigação de delitos cibernéticos, os quais podem ser praticados em qualquer parte do mundo. Além disso, começou a se tornar evidente a urgência de promulgar leis que abordassem especificamente os crimes cometidos no âmbito digital, que apenas surgiria no país muitos anos depois.

1.3 CLASSIFICAÇÕES DOS CIBERCRIMES

A tarefa de classificar esses crimes no código penal não é simples e direta. Isso se deve ao fato de que a tecnologia está em constante evolução, passando por mudanças rápidas e constantes. Essa dinâmica implica que as avaliações e perspectivas dos legisladores sobre o assunto também estejam sujeitas

a frequentes alterações. No entanto, apesar da complexidade, a classificação desses crimes permanece como um tema ativo, fundamentado no bem jurídico protegido pela lei penal.

Pinheiro (2021) classifica os crimes cibernéticos em virtuais puros, mistos e comuns. O crime virtual puro seria qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, pelo atentado físico ou técnico ao equipamento, inclusive dados e sistemas. Crime virtual misto, seria aquele em que o uso da internet é indispensável para a efetivação da conduta, e tem como fim algum bem da vítima, como, por exemplo, as transferências ilegais de valores, roubo de dados, já os crimes virtuais comuns são os crimes “tradicionais” que se aproveitam da internet para praticá-lo, como a disseminação de ofensas raciais.

Alguns autores dividem também os crimes virtuais de forma distinta, sendo crimes cibernéticos próprios ou impróprios, onde os crimes próprios serão aqueles que a legislação tipifica que a prática delituosa deve ocorrer pelo meio virtual, e o crime virtual impróprio, onde o delito será praticado por meio virtual, mas não existe uma tipificação específica para o local que o delito vá ocorrer. Os crimes virtuais impróprios, em grande parte não necessitam de conhecimentos técnicos de informática pelo agente do delito, são aqueles tipificados, no Código Penal, pois violam bens jurídicos comuns. Relativamente aos crimes cibernéticos impróprios, muitas dessas condutas são punidas com respaldo no Código Penal de 1940.

Ademais, os cibercrimes podem ser praticados por uma multiplicidade de agentes, podendo ocorrer, inclusive, múltiplos delitos podem ocorrer simultaneamente. Esses criminosos têm a capacidade de estar em diferentes locais ao mesmo tempo, dentro do ambiente virtual, não necessitando contato físico com a vítima.

2 ESPECIES DE CRIMES VIRTUAIS

Devido à constante inovação tecnológica e à adaptação dos criminosos cibernéticos, surgem inúmeras espécies de crimes cibernéticos. Dado que o crime cibernético não precisa de contato físico entre a vítima e o agente, acontecendo em um cenário frequentemente desprovido de presença humana, autoridade do governo ou território físico, não gerando inicialmente qualquer sensação de violência, e não existindo padrões predefinidos para que ocorra (Sydom, 2009).

Os crimes virtuais eram inicialmente voltados apenas para a sabotagem de sistemas, entretanto com o avanço do uso da internet pelo mundo, onde cada vez mais pessoas passaram a utilizá-la, os crimes cibernéticos tiveram uma rápida evolução, expandindo também as formas em que delitos podem ser praticados através da rede de internet.

É desafiador verificar a prática de comportamentos criminosos no âmbito virtual, uma vez que identificar o agente responsável não é uma tarefa simples, visto que algumas condutas possuem características específicas, que precisam de uma análise mais detalhada para uma precisa classificação no âmbito penal. Para que assim seja possível adotar medidas apropriadas.

Diante das vastas espécies, as que se destacam entre os autores são os crimes cibernéticos contra a honra, crimes de invasão de privacidade e intimidade, estelionato, crimes sexuais envolvendo menores e a violência virtual contra a mulher. As espécies de crimes virtuais que em sua grande maioria trata-se de crimes virtuais impróprios, uma vez que não existe lei específica para tal conduta feita online, sendo necessário o uso de outras legislações.

2.2 CRIMES CONTRA A HONRA

A honra é considerada um direito fundamental, resguardado pela constituição. Refere-se às características, particulares, tanto físicas quanto morais e intelectuais, de um indivíduo, que contribuem para seu respeito perante a sociedade. A honra desempenha um papel crucial na determinação da aceitação de um indivíduo em um determinado grupo social, sendo, assim, um ativo pessoal que merece proteção (Crespo, 2011).

Pode ser classificada em objetiva e subjetiva, a honra objetiva trata da opinião de terceiro sobre características morais, intelectuais e físicas de alguém,

refere-se a índole perante a sociedade, já a honra subjetiva é aquela opinião que se tem sobre si mesmo e suas características, sem se importar com opiniões de terceiros (Capez, 2019).

Os crimes contra a honra são divididos em três tipos pela legislação penal brasileira.

> **Calúnia**
> Art. 138 Caluniar alguém, imputando-lhe falsamente fato definido como crime: Pena - detenção, de seis meses a dois anos, e multa.
> **Difamação**
> Art. 139 Difamar alguém, imputando-lhe fato ofensivo à sua reputação: Pena - detenção, de três meses a um ano, e multa.
> **Injúria**
> Art. 140 Injuriar alguém, ofendendo-lhe a dignidade ou o decoro: Pena - detenção, de um a seis meses, ou multa (Brasil, 1940).

O delito de calúnia configura-se quando há a conduta específica de atribuir, de maneira falsa e intencional, a prática de um ato definido como crime a alguém, resultando na mancha da reputação dessa pessoa perante a sociedade. Já o crime de difamação ocorre ao simplesmente imputar qualquer adjetivo que venha a ofender a reputação de um indivíduo em particular. Nesse caso, o delito atinge a honra objetiva do sujeito por meio da ação de terceiros, que desempenham o papel de agentes ativos do crime, alterando a imagem do indivíduo perante a sociedade. A injúria, por sua vez, tinge a honra subjetiva ao ofender a dignidade e o decoro íntimo do indivíduo. Neste caso, não é necessário que terceiros tenham conhecimento, bastando que o ofendido se sinta menosprezado e ultrajado pelo proferimento da ofensa.

No ambiente virtual, tais crimes tem se tornado uma crescente preocupação entre os usuários, se tornando cada vez mais frequente o ingresso de ações judiciais envolvendo crimes virtuais contra a honra, uma vez que as redes sociais proporcionam um espaço para uma rápida propagação de informações difamatórias, caluniosas ou injuriosas que podem impactar diretamente a reputação e a dignidade dos indivíduos, esses crimes podem ser praticados através de comentários, mensagens e postagens do agente.

Atualmente, através de suas redes sociais, as pessoas passaram expressar suas opiniões sem receio de qualquer consequência, escondendo-se do que acreditam que seja uma mera liberdade de expressão.

A base da liberdade de expressão está intrinsecamente ligada à autonomia e dignidade humanas, exigindo o respeito pelos direitos fundamentais. As tecnologias da informação proporcionam uma nova perspectiva à liberdade de expressão, destacando de maneira positiva o aumento da participação social e a interação cultural, o que contribui para o acesso a uma democracia genuína (Pannain; Pezzella, 2015).

Entretanto, a liberdade de expressão é entendida como o direito de manifestar livremente opiniões, pensamentos e ideias, mas encontra limitações conforme estabelecido em nossa legislação. Embora cada indivíduo tenha o direito à sua opinião, é crucial reconhecer que a manifestação dessa opinião poderá gerar responsabilidade, uma vez que não são todas as manifestações de opinião que tem proteção legal. Assim, as publicações contendo conteúdos ofensivos nas redes sociais, aplicativos e outros meios virtuais estão sujeitos a ações judiciais, desde compensações por danos morais ou materiais, assim como processos criminais

É crucial entender que as redes sociais e aplicativos possuem um amplo alcance público, ampliando ainda mais a exposição da pessoa afetada, os danos causados e suas consequências. E por isso a utilização de computadores e recursos online, juntamente com outros recursos usados para os usuários cometerem delitos, levou o Estado a reconheceu sua falta de preparo para efetivamente julgar e penalizar esses potenciais criminosos, onde frequentemente resultam em danos à reputação de terceiros (Silva; Bezerra; Santos, 2016).

Com esse reconhecimento, em 2019, foi adicionada uma nova agravante aos crimes contra a honra na legislação brasileira feitos no ambiente virtual, aplicando o tripo da pena nos casos em que o crime é cometido ou divulgado em quaisquer modalidades das redes sociais da rede mundial de computadores, prevista no §2º, do artigo 141 do código penal.

2.3 CRIMES DE INVASÃO DE PRIVACIDADE E INTIMIDADE

Assim como o direito a honra, o direito à privacidade e intimidade tem proteção constitucional, previstos no artigo 5°, X, estão inseridos no roll de direitos fundamentais, a conduta foi inserida no Código Penal, através da Lei nº 13.737 de

2012 conhecida popularmente como Lei Carolina Dickmann, quando se fala em invasão de dispositivos informáticos.

Os bens jurídicos protegidos são a intimidade, a vida privada e o direito ao sigilo de dados contidos em dispositivos informáticos, sendo essencial primeira parte da tipificação penal encontra-se o ato de "invadir", que se refere a ingressar virtual sem a autorização explícita ou implícita do titular do dispositivo. Não é essencial a ocorrência de alterações, obtenção ou destruição de dados, ou informações. A segunda modalidade do delito, caracterizada pelo termo "instalar", configura-se pela simples introdução de vulnerabilidades, sem a necessidade da efetiva obtenção de vantagem ilícita, caracterizando assim um crime formal (Capez, 2016).

Com a lei n° 13.737, foi acrescida a legislação uma importante qualificadora, que está ligada diretamente com a invasão à intimidade da vítima, onde a invasão que resultar em obtenção de informações privadas e sigilosas, terá um aumento na pena, com a ressalva de sua não incidência em caso prática de crime mais grave, tendo também uma majorante, ligada a essa qualificadora, onde a pena é aumentada de um a dois terços em casos que ocorram divulgação, comercialização a terceiros, das informações ou dados obtidos pela invasão (Capez, 2016).

2.4 ESTELIONATO VIRTUAL

Um dos delitos que teve aumento significativos nos últimos anos com a popularização dos dispositivos informáticos foi o de estelionato, o principal crime quando se fala sobre a inviolabilidade patrimonial. O Código penal brasileiro prevê em seu artigo 171, o estelionato como:

> Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento: Pena – reclusão, de quatro a oito anos, e multa (Brasil, 1940).

O crime é consumado com a obtenção de vantagem ilícita indevida, prejudicando terceiros. Induzir ou manter a vítima em erro caracteriza um crime doloso, evidenciando a clara intenção de induzir ou manter alguém ao erro, para que a vítima de forma “voluntaria” o bem pretendido ao agente, no âmbito virtual, é bastante comum a utilização de links enviados por e-mail, mensagens de texto ou

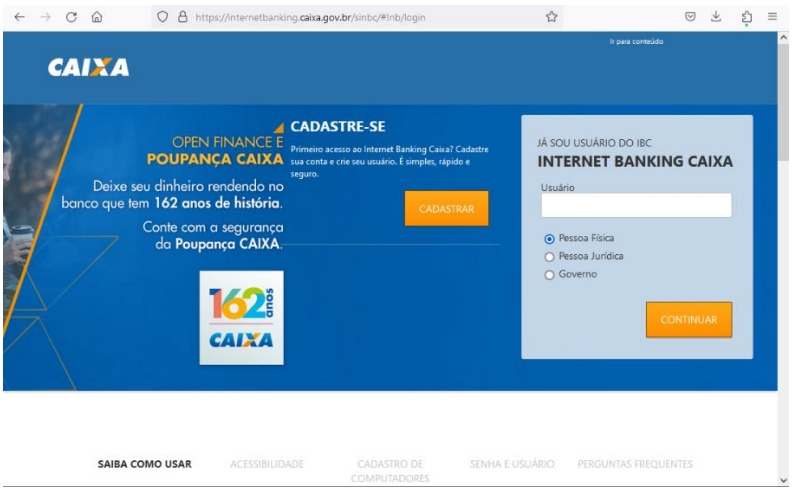
por meio de redes sociais como o Whatsapp e Instagram, contendo conteúdo enganoso que o intuito de enganar os usuários, prática conhecida com Phishing, induz os usuários a clicarem no link enviados, redirecionando-os para um site falso que solicita informações pessoais e/ou bancárias. Esse processo permite que o criminoso se aproprie desses dados e, posteriormente, os utilize para transferir valores disponíveis em contas bancárias para sua posse ou realizar compras em nome da vítima.

Normalmente o Phishing entram em contato com suas vítimas como se fossem instituições bancárias informando supostas transações suspeitas ou solicitando que dados sejam atualizados, embora na maioria das vezes o intuito seja enganar os usuários para fornecer informações, há casos onde arquivos, que se baixados são capazes de obter informações do dispositivo e danificar dados, são anexados em conjunto com as mensagens.

Uma outra modalidade de estelionato virtual envolve a criação de sites falsos que apresentam aparência e registro semelhantes aos originais, com o objetivo de capturar os dados dos usuários. Essa prática é denominada Typosquatting, onde os agentes criam uma página na web idêntico a de grandes e conhecidas empresas (Barreto, 2021).

Nessa situação, a plataforma falsa que foi criada não tem qualquer ligação com a empresa original. E ao repassar informações pessoais como nome de usuário, senha ou número do cartão de crédito, os criminosos são capazes de obter dados para serem utilizados posteriormente.

Figura 2 – Site original do Internet Banking Caixa



Fonte: Caixa (2023).

Figura 3 – Site com prática de Typosquatting do Internet Banking Caixa

Fonte: NoliCorp (2015).

Outra prática que vem crescendo, envolve a clonagem de números de telefone, resultando em um crime no qual os criminosos se passam por pessoas conhecidas da vítima, solicitam transferências de dinheiro e a persuadem a efetuar os pagamentos desejados em suas contas. Pesquisa levantada pela empresa especializada em segurança digital, Psafe, realizada no ano de 2019, informa que pelo menos 8,5 milhões de brasileiros, cerca de 23 vítimas diárias, já tiveram o aplicativo de mensagens instantâneas, WhatsApp, clonado. Também é frequente de golpes sem o uso de clonagem, nos quais os criminosos, por meio de outros números telefônicos, se apresentam como conhecidos da vítima, alegando terem perdido ou trocado de número.

Esse estratagema visa enganar a vítima, que pode não reconhecer o novo e desconhecido número. Assim, evidencia-se que, à medida que a internet se expande e as redes sociais, juntamente com seus sistemas de proteção, se aprimoram, novas formas de crimes virtuais continuam a ser desenvolvidas.

Atualmente, é evidente o crescimento das atividades criminosas ocorrendo por meio digital, em especial o estelionato, através de dados fornecidos na nova edição do Anuário Brasileiro de Segurança pública, mediante dados de boletins de ocorrências coletados, golpes aplicados pela internet aumentaram 65,2% no ano de 2022 comparado com o ano anterior, o número de estelionatos virtuais foi de 200.322, número que podem ser ainda maiores, uma vez que seis estados não especificaram o delito virtual cometido, uma vez que o estelionato virtual foi tipificado apenas no ano de 2021, pela criação da PL 4.554/2020, que resultou na lei 14.155 de 2021 no qual prevê a modalidade qualificada dos crimes de furto e estelionato

quando cometidos por meio da internet, resultando no aumento da pena para essas infrações.

2.5 CRIMES CONTRA A LIBERDADE SEXUAL DE MENORES

A globalização introduziu avanços tecnológicos que anteriormente eram inimagináveis, proporcionando à humanidade uma rapidez sem precedentes nos meios de comunicação. Isso permitiu às novas gerações terem acesso fácil a uma ampla gama de informações por meio da internet em questão de segundos. Com tais avanços, as crianças atualmente já crescem inseridos no mundo digital, e em conjunto com o distanciamento social decorrente da pandemia da Covid-19, as redes sociais tornaram-se o principal meio de entretenimento para muitas crianças e adolescentes, e assim criando um terreno propício para a ocorrência de crimes envolvendo menores.

A prática desse crime é predominantemente realizada por meio da Internet, devido à sua facilidade de utilização e acesso. Em plataformas de redes sociais, os perpetradores muitas vezes empregam perfis falsos e uma linguagem mais juvenil, criando uma falsa sensação de segurança.

No âmbito virtual, são frequentemente cometidas diversas condutas criminosas contra criança e adolescente, especialmente aquelas relacionadas aos crimes contra a liberdade sexual desses indivíduos (Capez, 2016).

No ambiente virtual, as condutas mais destacadas são aquelas descritas nos artigos 241-A e 241-B do Estatuto da Criança e do Adolescente. O artigo 241-A aborda punições para práticas ilícitas relacionadas à disseminação de imagens de sexo explícito ou pornografia envolvendo crianças e adolescentes. Enquanto isso, o artigo 241-B penaliza quem obtém, de qualquer maneira, possui ou armazena qualquer imagem ou fotografia que contenha cenas de sexo explícito ou manifestação de pornografia envolvendo criança e/ou adolescente (Capez, 2016).

E somente nos casos estabelecidos pelo Estatuto da Criança e do Adolescente encontramos normas penais voltadas para a proteção de crianças e adolescentes nos casos de abuso sexual virtual, entretanto não exista uma diferenciação entre tipos penais ao que se refere a ser praticado no ambiente físico ou virtual.

No dia 12 de abril de 2023, foi promulgado um decreto que oficializa a adesão do Brasil à Convenção de Budapeste, a qual aborda questões relacionadas

a crimes cibernéticos e impõe obrigações específicas no combate à pornografia infantil. E com isso é esperado que em breve ocorram modificações na legislação brasileira com o intuito de aprimorar a regulamentação dessa prática.

2.6 VIOLÊNCIA CONTRA A MULHER

Em 2006, entrou em vigor a Lei 11.340/06, que estabeleceu mecanismos para combater a violência contra as mulheres, especialmente no contexto doméstico, seja cometido por um parceiro com quem houve relação afetiva ou por um parente com quem a mulher agredida compartilhe convivência. Essa legislação ficou popularmente conhecida como Lei Maria da Penha, devido ao caso da farmacêutica Maria da Penha Maia Fernandes, que por quase duas décadas foi vítima de violência por parte de seu marido, chegando ao ponto de ficar paraplégica após ser alvejada por um tiro de espingarda disparado por ele (Cunha, 2015).

A violência contra a mulher pode ocorrer de várias formas, física, patrimonial, moral, sexual, psicológica, etc. Todas são condutas já tipificadas pela Lei Maria da Penha, entretanto, a violência contra as mulheres é bem mais complexa. Além de serem vítimas no mundo físico, as mulheres enfrentam uma significativa incidência de diversas formas de violência no ambiente virtual.

No cenário em que a disseminação de conteúdo ofensivo ou prejudicial é facilitado pelo mundo virtual, as mulheres tornaram-se as principais vítimas. Nesse contexto, a violência praticada torna-se tão cruel quanto uma agressão física ocorrida no ambiente doméstico.

Com o progresso tecnológico das últimas décadas e a disseminação generalizada do uso de novas tecnologias, como internet, redes sociais e smartphones, a violência contra as mulheres adquiriu uma ferramenta implacável. Diariamente, inúmeras mulheres em todo o país são alvo de diversas formas de violência, em todos os aspectos diários, da vida pessoal a vida profissional, a internet tornou-se uma ferramenta para a prática de violência, sem que seja estabelecido um mecanismo eficaz para lidar com essa nova manifestação de violência de gênero, frequentemente perpetradas por homens motivados por sentimentos de ódio, vingança ou objetivos financeiros. Essa violência vem tornando-se cada vem mais recorrente, algumas vezes por meio de comportamentos vistos como comuns, como a exigência de senhas do celular e redes sociais.

Novas formas de violência também surgiram com esse avanço tecnológico, entre essas novas condutas vem sendo crescente o delito de divulgação sem autorização de vídeos e imagens com conteúdo íntimo como forma de vingança, conduta conhecida como revenge porn ou pornografia de vingança, uma forma de violência moral com cunho sexual, surge também o estupro virtual e a extorsão, este último tendo como finalidade obter vantagem financeira mediante chantagem.

Nesse contexto, Recupero (2016):

> A “pornografia de vingança” tipicamente se refere à disseminação (sem o conhecimento ou consentimento do sujeito) de mídia sexualmente explicita, como fotos ou vídeos, que foram originalmente obtidos com o consentimento do sujeito, geralmente originada de um relacionamento íntimo romântico.

No estado do Espírito Santo, nos últimos anos, foram registrados diversos casos na Delegacia de Repressão aos Crimes Cibernéticos. Esses casos apresentam, em grande parte, um padrão de comportamento criminoso semelhante. Após o término de um relacionamento amoroso, homens, inconformados com a separação e impulsionados por sentimentos possessivos, costumam divulgar imagens íntimas da ex-parceira, capturadas durante o período em que havia comprometimento e confiança mútua no relacionamento. (Azeredo; Carlos; Wendt, 2016)

Normalmente, os agentes desse crime de compartilhamento não autorizado de fotos íntimas de mulheres são parceiros íntimos, familiares, amigos ou mesmo desconhecidos. No entanto, há uma ênfase significativa nos ex-parceiros, que, muitas vezes, sentindo-se contrariados pelo término do relacionamento, buscam vingança ao divulgar imagens íntimas das ex-companheiras como uma maneira de puni-las por não querer mais manter o vínculo afetivo (Barreto, 2017).

Nesse sentido, foi criada a Lei nº 13.718, de 24 de setembro de 2018, que pune com mais rigor a divulgação de fotos íntimas, não autorizadas, de mulheres que tenham mantido relação íntima de afeto com os responsáveis pela divulgação. É importante destacar que, até entrada em vigor desta lei, a divulgação de fotos íntimas não era considerada um crime específico, até essa data, expor imagens íntimas de ex-namoradas, ex-esposas, ex-companheiras ou qualquer outra

mulher maior de 18 anos era enquadrado apenas como crime de injúria, uma infração penal considerada de menor potencial ofensivo.

Entre os crimes patrimoniais contra mulher, com a era digital também surgiu os chamados Scammers, indivíduos especializados em se aproximar de mulheres através de redes sociais, visando obter vantagens financeiras de maneira criminosa, identificados como "Golpistas da Nigéria". Esse termo é utilizado porque essa prática é frequentemente associada a pessoas desse país, onde o governo enfrenta desafios para rastrear os criminosos. Após perpetrar os golpes, esses fraudadores desaparecem e criam novos perfis, continuando assim a aplicar novos golpes em outras vítimas (Stoco, 2018).

O principal instrumento para enfrentar à violência doméstica e familiar contra as mulheres é a Lei nº 11.340/2006. Legislação de extrema importância não apenas estabelece e classifica as diferentes formas de violência contra as mulheres, sendo física, psicológica, sexual, patrimonial ou moral, ela também estabelece a criação de serviços especializados. Estes serviços fazem parte da Rede de Enfrentamento à Violência contra a Mulher, envolvendo instituições relacionadas à segurança pública, justiça, saúde e assistência social.

Entretanto, ao tratar da violência contra a mulher no ambiente virtual, ainda são escarças as políticas públicas e legislações apropriadas para o enfrentamento dessas condutas que vem sendo cada vez mais presente na sociedade.

3 LEGISLAÇÃO NACIONAL SOBRE CIBERCRIMINALIDADE

Os avanços na tecnologia da informação têm provocado mudanças significativas na sociedade contemporânea, resultando em uma crescente disparidade entre as instituições estabelecidas do sistema jurídico convencional e as abordagens inovadoras exigidas para atender às demandas desta era moderna (Pinheiro, 2021).

Leis que estabeleçam os direitos dos usuários da Internet e deveres dos prestadores de rede são fundamentais para que o Judiciário possa lidar com violações e riscos inerentes a sociedade da informação, e, sobretudo, de modo a evitar decisões contraditórias e injustiças diante de casos concretos. Legislações regulatórias da Internet são apontados como fatores que fortalecem a sociedade na era da informação, nas dimensões, social, cultural e econômica, e vêm sendo estudados em todo o mundo (Carvalho, 2014).

O Brasil adota o sistema da reserva legal, seguindo o princípio da legalidade, são preceitos fundamentais do direito que determinam que não será considerado delito ou passível de pena conduta que não tenha lei prévia que a defina.

Entretanto, conforme relatado por Jesus e Milagre (2016), no Brasil, deferente dos outros países, adotou-se primeiro a legislação penal, que deveria ser a *ultima ratio*, antes do surgimento de legislações adequada frente as condutas ilícitas nos meios informáticos, e Leis como a n° 12.965 de 2014, denominada “Marco Civil da Internet”, e as Leis 12.735 e 12.737 ambas de 2012, mesmo com poucos artigos, ainda trazem inúmeros pontos omissos.

As autoridades judiciais e de investigação enfrentaram desafios na identificação dos responsáveis pelos crimes cometidos em ambientes virtuais, devido às peculiaridades e inovações dos meios tecnológicos e da internet. Essas características acabaram facilitando a fuga e a ocultação da autoria. Esse cenário é agravado pelo elevado número de usuários dessa nova tecnologia e pela possibilidade de fornecer informações falsas sobre o endereço de IP, dificultando a rastreabilidade dos perpetradores (Siqueira, 2017).

Os crimes virtuais, têm se tornado uma preocupação crescente para a sociedade e, consequentemente, para a legislação, é notório os seus danos

causados a sociedade e a economia, diante da dificuldade da legislação brasileira ao tratar de crimes cibernéticos.

3.1 LEIS 12.737 DE 2012

A Lei n° 12.737 de 2012, conhecida como Lei Carolina Dieckmann, foi um marco importante na legislação brasileira, trata-se da primeira lei brasileira criada para combater e penalizar crimes no campo da cibecriminalidade, trouxe alterações no Código Penal Brasileiro, e é considerada até hoje como a principal ferramenta legal para a segurança virtual no Brasil.

O projeto de lei 2.793/2011 que acrescentava ao Código Penal o artigo 154-A, no qual trazia a tipificação da conduta de invasão de dispositivo informático, que foi proposto devido a episódios de ataques a sites do governo, os deixando instáveis e outros inúmeros casos de delitos virtuais, ganhou notória atenção, quando a atriz Carolina Dieckman foi vítima de exposição íntima na internet, ao ter seu computador invadido, e ter 36 fotos íntimas divulgadas após não ceder a uma tentativa de extorsão, onde os criminosos exigiam a quantia de dez mil reais para a não divulgação do material.

Os autores do projeto argumentavam que as anteriores propostas de criminalização, presentes em outros projetos, eram excessivamente amplas e desproporcionais. Elas não eram capazes de categorizar criminalmente comportamentos comuns praticados pelos usuários da internet. Além disso, essas propostas tipificavam assuntos como o armazenamento e acesso a registros de conexão, os quais deveriam ser abordados em diretrizes mais abrangentes e cuidadosas com os direitos dos cidadãos, sendo assim o projeto apresentava notórias diferenças em relação a PL que resultou na Lei Azeredo.

Conforme a justificativa do Projeto, que se transformou na Lei 12.737/12, fica evidente que a maioria das definições de crimes propostas anteriomente apresentava uma linguagem amplamente aberta. Frequentemente, essas definições se enquadram como condutas em si, sem depender do resultado ou da intenção específica do agente. Essa abordagem redacional se alinha com uma sociedade preocupada com riscos e uma lógica de direito penal que se assemelha ao "inimigo". Buscavam antecipar a proteção penal para fases anteriores à ocorrência de danos, o que inclui flexibilizar as regras de causa e efeito, classificar comportamentos que são considerados insignificantes, impor penas mais severas e desproporcionais, e criar

crimes de perigo abstrato, entre outras características. Um exemplo disso é a criação de um capítulo que visa legalmente proteger a "segurança dos sistemas informatizados" como um bem jurídico. Essa abordagem, abre a possibilidade de aplicar penalidades graves a ações que, por sua natureza ou intenção, não justificariam uma resposta penal, como o acesso não autorizado a sistemas de computadores resultante de testes de segurança realizados sem o consentimento prévio dos proprietários dos sistemas (Jesus; Milagre, 2016).

Sabe-se que o processo de aprovação e vigência de leis no Brasil costumam ser demorado. No entanto, neste caso em particular, foi diferente, pois a legislação foi aprovada em tempo recorde. Tal caso ocorreu devido a forte pressão da mídia sobre as autoridades, por a vítima tratar-se de uma figura pública muito conhecida. O incidente de vazamento das fotos ocorreu em maio de 2011, quando um hacker conseguiu acessar o computador pessoal da atriz.

A lei inseriu os artigos 154-A e 154-B ao Código Penal, criando a “invasão de dispositivo informático”, regulamentando sua ação penal, e penalizando em detenção e multa para aquele que invadir dispositivo informático pertencente a terceiros, independentemente se esteja ou não conectado à rede de computadores, com o objetivo de adquirir, modificar ou eliminar dados ou informações sem a devida autorização explícita ou implícita do usuário do dispositivo, ou instalar vulnerabilidades com a intenção de obter vantagens de forma ilícita.

Qualquer pessoa pode praticar o crime de invasão de dispositivo informático, uma vez que o delito não exige nenhuma condição especial. Já o sujeito passivo pode ser o proprietário do aparelho informático invadido ou qualquer outra pessoa que tenha inserido informação ou dados neste dispositivo. A conduta necessária para a configuração do delito consiste no ato de ‘’invadir’’ que significa ingressar virtualmente, sem a concordância expressa ou tácita do proprietário do dispositivo. Onde o objeto material do crime é o dispositivo informático alheio.

Invasões de dispositivos informáticos, podem afetar uma variedade de vítimas, a depender dos objetivos dos invasores, as vítimas vão desde indivíduos comuns, a empresas, instituições financeiras e governo. Conforme dados coletados pela empresa multinacional, Fortinet, que desenvolve e comercializa produtos e serviços para soluções em segurança cibernética, o Brasil, no primeiro semestre de 2022, ficou atrás apenas do México, entre os países da América Latina, que mais sofreram ataques cibernéticos, registrando cerca de 31,5 bilhões de tentativas de

invasão por ataques virtuais contra empresas que usam os recursos de segurança digital da Fortinet, número 94% maior se comparado com os dados colhidos do mesmo período no ano de 2021.

Embora a Lei Carolina Dieckmann tenha um papel importante na legislação no Brasil, ao analisá-la, é fácil identificar deficiências em certos aspectos que deveriam contribuir para alcançar seu principal objetivo. Seja no que diz respeito à obtenção de evidências ou à imposição de punições, a lei apresenta lacunas significativas que a impedem de oferecer proteção amplamente adequada, a principal crítica recai sobre o que é disposto no artigo 154-A do Código Penal, onde apenas será considerado crime nos casos em que houvesse invasão de um dispositivo com algum mecanismo de segurança. Em outras palavras, se a vítima não tiver medidas como antivírus, firewalls, senha ou qualquer outro meio que garanta a segurança de seu dispositivo eletrônico e, ocorrer uma violação virtual, essa ação não será considerada como invasão de dispositivo informático. Isso ocorre porque é necessário ter contornado algum tipo de mecanismo de segurança para que o ato seja enquadrado como tal.

Outra crítica ao mesmo artigo, é sua não abrangência a situações em que alguém invade um computador ou qualquer dispositivo móvel simplesmente com a intenção de realizar uma invasão, sem o intuito de obter vantagem ilícita. Nesses casos, não seria considerado crime, uma vez que o objetivo do autor é apenas “explorar”. A lei permite a simples invasão não é passível de punição.

Existiam várias maneiras pelas quais a invasão de dispositivos eletrônicos poderia ocorrer sem que o responsável seja punido, devido à deficiência encontrada na legislação que não se adequavam à certas essas situações. Além disso, crimes cibernéticos requerem evidências, especialmente em termos de perícia, uma vez que é difícil obter testemunhas para esse tipo de delito.

3.2 LEI N°12.735 DE 2012

Não muito popular, a Lei n° 12.735 de 2012, que ficou conhecida como Lei Azeredo, trouxe a tipificação das condutas realizadas mediante o uso de sistemas eletrônicos, digitais ou similares contra sistemas informáticos, mas não acrescentou nenhum tipo penal ao ordenamento jurídico, e estabeleceu a possibilidade dos órgãos da polícia judiciaria estruturarem setores e equipes

especializadas no combate aos delitos em redes, dispositivos e sistemas informáticos e de comunicações.

Seu projeto de lei é de 1999, mas no período foi duramente criticada pelos defensores de liberdade na rede, sendo até mesmo apelidado de AI-5 digital, devido à pressão ocorreu a retirada da maior parte de seus artigos, atualmente boa parte da lei foi vetada.

3.3 LEI N° 12.956 DE 2014

Diante da necessidade de regulamentar a internet sem infringir direitos e liberdades, em 29 de junho de 2009, foi iniciado um processo de construção colaborativa e democrática entre a sociedade e o governo. Esse esforço foi liderado pela Secretaria de Assuntos Legislativos do Ministério da Justiça, em parceria com a Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas. Realizado por meio da internet, esse processo estabeleceu as bases para o Marco Civil, que culminou no projeto de Lei nº 2.126/11.

Após um longo período, o projeto de Lei 2.126/11, foi sancionado pela Presidência da República em 23 de abril de 2014, tornando-se a Lei N°12.956 de 2014, conhecida como Marco civil da internet, trata-se de norma legal que disciplina o uso da internet no Brasil, por meio da previsão de princípios, garantias, direitos e deveres para quem faz uso da rede, bem como da determinação de diretrizes para a atuação do Estado.

> Marco civil da internet é considerado a “constituição da internet”, garantindo direitos e deveres a todos os atores da internet Brasileira usuários, provedores de conexão e de serviços em geral. Fruto de um projeto nascido em 29 de outubro de 2009, da secretaria de Assuntos Legislativos do Ministério da Justiça, em parceria com a Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas, o Marco civil foi uma construção colaborativa, disponível para consulta pública entre novembro de 2009 e junho de 2010, tendo recebido mais de duas mil contribuições1. Após a fase de participação popular, ingressou no congresso em 24 de agosto de 2011, por meio do Projeto de Lei n. 2.126, de iniciativa do Poder Executivo, projeto que visou estabelecer princípios, garantias, direitos e de- veres para o usuário da internet no Brasil. A legislação tem escopo de evitar, igualmente, decisões contraditórias proferidas pelo Judiciário, em casos semelhantes envolvendo tecnologia da informação, gerando insegurança jurídica. Foi sancionado pela Presidência da República em 23 de abril de 2014, tornando-se a Lei n. 12.965. Cogita-se, ainda, da propositura na Assembleia das nações Unidas de um possível Marco civil internacional. O Marco civil da internet pode ser integrado s leis e Projeto de estudo neste livro. São complementares nas atividades envolvendo repressão a crimes cibernéticos (Jesus, 2016).

Siqueira (2017) expõe que Marco Civil foi estabelecido para preencher as lacunas no sistema jurídico relacionadas aos crimes virtuais. Em sua primeira fase, a lei aborda os fundamentos, conceitos para interpretação e os objetivos que a orientam. Além disso, ela enumera os direitos dos usuários, lida com questões polêmicas, como a solicitação de históricos de registros, delineia a atuação do poder público diante dos crimes virtuais e, por fim, assegura o exercício do direito dos cidadãos de utilizar a internet de maneira individual e coletiva, com devida proteção legal.

Conforme destacado por Souza (2021), o objetivo fundamental do Marco Civil da Internet é preservar a privacidade dos usuários, visando garantir a confidencialidade e a intocabilidade das comunicações, conforme preconizado pela Constituição Federal.

Uma das principais característica da legislação é a defesa da neutralidade da rede, onde os provedores devem tratar todos os dados em sua rede de forma igual, sem qualquer discriminação de conteúdo, origem, destino ou serviço, também estabelece a proteção da privacidade dos usuários, obrigando os provedores de internet proteger o registro de suas atividades e de seus usuários, pois é evidente que sem a colaboração dos provedores de internet ou de serviços informáticos torna a identificação dos autores dos delitos virtuais uma tarefa bem mais desafiadora.

Outro ponto de grande importância que a legislação trouxe tratar sobre a responsabilidade dos provedores sobre a publicação de conteúdos de terceiros, onde o provedor não será responsabilizado, a menos que não cumpra ordem judicial específica. E assim o Marco Civil apresenta três pilares, a garantia da neutralidade da rede, a proteção à privacidade dos usuários e a garantia de liberdade de expressão, respeitando os limites legais.

3.4 LEI 13.709 DE 2018

A Lei 13.709 de 2018, a Lei Geral de Proteção de Dados, LGPD, é a norma brasileira que tem como foco a regulamentação do tratamento de dados pessoais por organizações públicas e privadas no Brasil, veio como uma forma de complemento ao marco civil da internet, atendendo às exigências atuais referentes à segurança e preservação de dados tanto em ambientes online quanto offline.

A lei surgiu no país pela influência do Regulamento Geral da União Europeia sobre proteção de dados, a GDPR, que r presentou um dos momentos mais significativos na evolução no tratamento de dados pessoais, ao estabelecer em suas diretrizes que os estados-membros da União Europeia teriam a liberdade de realizar transações comerciais ou oferecer serviços que envolvessem dados pessoais, contanto que a legislação do outro país fosse, razoavelmente semelhante à deles. Essa imposição serviu como estímulo para que diversas nações revissem ou criassem novas abordagens no tratamento de dados pessoais, influenciando também empresas por todo o mundo, inclusive grandes como google, a modificares a forma no qual coletavam e tratavam dados.

Os principais fundamentos da LGPD são, a proteger a privacidade envolve garantir os direitos essenciais, como a preservação da intimidade, honra, imagem e vida privada. Além disso, isso implica permitir que os cidadãos controlem e protejam seus dados pessoais e informações íntimas, promovendo a liberdade de expressão, informação, comunicação e opinião, direitos fundamentais da Constituição brasileira. Essas medidas não apenas asseguram a segurança jurídica em todo o país, facilitando o desenvolvimento econômico, tecnológico e a inovação, mas também promovem a livre iniciativa, a concorrência justa e a proteção do consumidor por meio de regras transparentes e aplicáveis em todo o território nacional. Também está em conformidade com os princípios dos direitos humanos, garantindo o livre desenvolvimento da personalidade, a dignidade e o pleno exercício da cidadania pelos indivíduos.

É essencial ressalvar que a lei atribui um valor significativo aos dados, reconhecendo-os como um dos elementos essenciais na formação da identidade humana. Isso visa criar um ambiente saudável no qual o desenvolvimento humano possa ocorrer de maneira a enriquecer a sua personalidade. Os dados, sendo de extrema importância, devem permanecer sob o controle exclusivo daqueles a quem pertencem. Qualquer tentativa de transferir esses dados para fora desse controle é considerada uma ameaça à integridade da personalidade e aos direitos fundamentais da pessoa.

3.5 LEI N° 13.772 DE 2018

Lei de grande importância na defesa da mulher, a Lei 13.772 de 2018, trouxe mudanças ao Código Penal e na Lei n°11.340 de 2006, a Lei Maria da Pena, reconhecendo que a violação da intimidade da mulher configura violência doméstica e familiar, criminalizando os registros de caráter íntimo e privado feitos sem autorização, gerando a pena de detenção de seis meses a um ano e multa.

Na mesma pena também irá incorrer para quem realizar montagens, seja de foto, video, áudio ou qualquer outro tipo de registro visando incluir pessoa em cena de nudez, sexual ou libidinoso de caráter íntimo.

3.6 LEI 14.155 DE 2021

A mais recente legislação brasileira ao tratar sobre crimes virtuais, a Lei 14.155, passou a vigorar em 2021, trazendo modificações nos Códigos Penal e Processual Penal brasileiro, tornando algumas punições mais severas os crimes de violação de dispositivos informativos, furtos e estelionato cometidos de forma eletrônica ou pela internet.

Para os crimes de furto, a nova lei trouxe a pena de reclusão de quatro a oito anos, quando realizado por meio de dispositivo eletrônico ou informático, conectados ou não à rede de computadores. Quanto ao crime de estelionato, este terá detenção de quatro a oito anos e multa quando a vítima for ludibriada e entregar seus dados através das redes sociais, contatos telefônicos ou qualquer meio fraudulento análogo e em crime de estelionato praticado contra idoso ou vulnerável, a pena para estelionato também cresce.

A lei trouxe uma nova redação ao tratar sobre invasão de dispositivos informáticos, introduzido no ordenamento brasileiro pela lei 12.737/21, onde a pena de detenção passou de três meses a um ano para de uma ano a quatro anos de detenção. Como já relatado a redação original trazida pela Lei 12.737/2012, era somente considerado crime, caso o invasor do dispositivo de uso alheio passasse por alguma “barreira”, ou seja, caso alguém não tivesse senha em seu dispositivo, ou tivesse passado a senha para outra pessoa, não se configurava como crime, porém, a redação foi alterada pela Lei 14.155/21, passando a considerar crime mesmo que o invasor não viole nenhum mecanismo de segurança.

Embora seja evidente a relevância dessa mudança quando se trata de controlar os delitos cometidos no ambiente cibernético, uma vez que esses crimes estão ocorrem cada vez com mais frequência, alguns doutrinadores apontam as omissões deixadas pelo legislador, uma vem que a substituição da expressão “mediante violação indevida de mecanismo de segurança” pelo termo “invadir”, não serve como base para a tipificação de qualquer acesso indevido, gerando ainda um cenário dúbio de aplicabilidade, e não existem subdivisões como ocorre na legislação de outros países para melhor aplicação da norma.

3.7 DECRETO Nº 11.491

Decreto publicado no dia 12 de abril de 2023, promulgou no Brasil a convenção sobre crimes cibernéticos, firmado em Budapeste.

A Convenção de Budapeste, também chamada de Convenção sobre Cibercrimes, foi estabelecida em 21 de setembro de 2001, na Hungria, após quatro anos de elaboração pelo Comitê de Peritos em Crimes no Ciberespaço, trata-se de um acordo internacional que abrange direito penal e direito processual penal, celebrado no contexto do Conselho da Europa com o propósito de fomentar a colaboração entre os países na luta contra crimes cometidos por meio da Internet e o uso de computadores.

A Convenção de Budapeste tem como objetivo principal harmonizar as leis penais substantivas, promover mudanças nas legislações processuais nacionais para facilitar investigações e persecuções criminais relacionadas a delitos cometidos por meio de sistemas de computadores, bem como outros crimes nos quais as evidências devam ser obtidas eletronicamente. Além disso, visa consolidar meios importantes de cooperação internacional.

Seu capítulo I traz algumas terminologias, definindo o que são sistemas e dados de computador, provedores de serviços e dados de tráfego.

Em seu segundo capítulo, traz as medidas a serem aditadas nas jurisdições nacionais, tratando em seu Título 1 sobre os crimes contra a confidencialidade, integridade e disponibilidade de dados e sistemas de computador e seus tipos, sendo eles acesso ilegal, interceptação ilícita, violação de dados, interferência em sistema e uso indevido de aparelhagem. No Título 2 encontram-se alguns crimes informáticos, dentre quais, falsificação informática e fraude informática. O Título 3 tratará de crimes relacionados ao conteúdo da informação,

abordando especificamente sobre pornografia infantil. Já no Título 4 discorre sobre violação de direitos autorais e de direitos correlatos. Outras formas de responsabilidade e sanções serão expostas no Título 5, nos casos de tentativa, auxílio ou investigação, e como ocorrerá a responsabilização penal para pessoa jurídica.

O Capítulo III, apresenta os princípios gerais da cooperação internacional, abordando os princípios relativos à extradição, a assistência mútua, informações espontâneas e os procedimentos relativos a pedidos de assistência mútua na falta de acordos internacionais aplicáveis, trazendo também os princípios referentes a confidencialidade e limitações de uso.

Por fim, a Convenção sobre Cibercrimes traz disposições sobre assinatura e vigência, adesão e efeitos da convenção, a aplicação territorial, declarações, cláusula federativa, reservas, status e retirada de reserva, emendas, solução de controvérsias, consultas entre as partes, denúncia e notificações.

Em resumo, a Convenção de Budapeste une internacionalmente países para um esforço em conjunto contra o cibercrime, estabelece três objetivos específicos, criar uma uniformidade nas leis penais no contexto cibernético entre os Estados signatários, definir os elementos do sistema de informática para promover uma interpretação consistente das leis penais internas e garantir a confiabilidade das provas eletrônicas no ambiente virtual e implementar um sistema ágil e eficiente de cooperação internacional para combater a criminalidade virtual.

CONSIDERAÇÕES FINAIS

Diante de todos os aspectos apresentados, buscou analisar a evolução tecnológica até o surgimento dos crimes cibernéticos e os impactos que esses delitos causaram na legislação brasileira, uma vez que os crimes cibernéticos têm assumido amplas proporções no Brasil e em todo mundo.

A internet e os meios de comunicação têm experimentado um crescimento exponencial, levando as pessoas a mudarem seus hábitos e se tornarem cada vez mais dependentes do mundo virtual, que influenciou diversos aspectos de suas vidas, de maneira sem precedentes, as consequências imediatas desse avanço, com o uso difundido de computadores e dispositivos eletrônicos pessoais e o acesso à vasta rede da digital, resultaram na consolidação desse meio de integração e comunicação em nossa sociedade.

Com um progresso tecnológico que visa simplificar a vida cotidiana, também aumenta a exposição à vulnerabilidade no mundo virtual, uso da tecnologia virtual não resultou apenas em benefícios para a sociedade atual. Com rápido e alarmante aumento no número de usuários, testemunhamos também o surgimento e disseminação de práticas criminosas, abrangendo aspectos pessoais, financeiros e políticos, esses delitos têm crescido de maneira significativa à medida que a internet se expande e se torna cada vez mais popular. Isso tem impactos significativos na sociedade, infringindo os direitos fundamentais dos cidadãos. Isso ocorre devido à facilidade com que os criminosos conseguem ingressar nesse ambiente e à dificuldade em identificá-los devido ao anonimato e à rapidez na destruição de evidências.

Cada vez mais, dados e informações pessoais estão susceptíveis a criminosos, que por vezes empregam técnicas avançadas para contornar os sistemas de segurança, e dessa forma, conseguem obter acesso a informações como dados bancários, senhas, fotos pessoais, vídeos, ou qualquer outro dado que possa proporcionar vantagens a eles. É crucial ressaltar essa problemática não afeta apenas a população, mas também o governo, empresas de diversos tamanhos e instituições financeiras, tornando o país como um todo mais suscetível às flutuações do mundo virtual. Sendo importante também desconstruir a ideia de que apenas pessoas com grandes conhecimentos tecnológicos são capazes de cometer crimes virtuais, muitas vezes, são cometidos por indivíduos com motivações diversas, que

vão desde o ganho financeiro até a simples satisfação pessoal, que apenas utilizam da facilidade e do anonimato do ambiente virtual para cometer crimes comuns.

A cada dia, novos dispositivos, redes sociais, aplicativos surgem, gerados novas oportunidades de prática criminosa através da internet, apresentando um desafio significativo. No Brasil isso se torna uma questão ainda mais crucial, uma vez que não há crime sem legislação que assim defina anteriormente, e não há pena sem prévia cominação legal. Inicialmente, os delitos perpetrados no âmbito virtual eram tipificados, por analogia. Dessa maneira, a conduta realizada no ambiente virtual era considerada de forma análoga à conduta prevista nos tipos comuns, visando evitar a impunidade do infrator cibernético. Entretanto, vários autores expressam sua objeção ao emprego, por analogia, nos casos de crimes praticados pela internet, uma vez que a analogia no âmbito penal não deverá ser usada in *malam partem*, que se fundamenta no princípio da taxatividade.

É compreensível a complexidade necessária na investigação e na elaboração de leis para enfrentar certos crimes virtuais, especialmente dado o caráter recente e dinâmico desse cenário e por conta da tecnologia estar em constante evolução, e novas práticas ilícitas continuam surgindo nesse ambiente de forma rápida. É nítido que ao longo dos anos a legislação brasileira passou por diversas alterações e adições para lidar com os desafios trazidos pela era digital. Sendo importante ressaltar avanços proporcionados como a Lei Federal n° 12.737/2012, conhecida como "Lei Carolina Dieckmann", e o "Marco Civil da Internet", promulgado pela lei n. 12.965/2014 e a mais recentemente, a Lei 14.155/21 que introduziu maior rigidez nas penalidades para os delitos de furto e estelionato. No entanto, embora haja complexidade para a elaboração, é notório a fragilidade e lacunas deixadas por essas mesmas leis.

São evidentes os desafios causados pela ausência de uniformidade nas penalidades e na falta de ferramentas especializadas para lidar com certas categorias de crimes virtuais, ainda são escassas as normas específicas voltadas para a proteção e punições contra crimes virtuais, o que cria obstáculos para a atuação da justiça. Visto que legislações importantes, como o Marco Civil da internet e a Lei de Proteção de Dados, não tratam sobre tipificações ou punições de condutas, sendo normas meramente reguladoras, já a lei 12.737 de 2012, apesar da sua importância, não consegue amparo efetivo, uma vez que traz lacunas e possibilidades de interpretações que facilitaram a impunidade dos delitos. Sendo

ainda necessário o uso de analogias ao Código Penal brasileiro para reprimir e resguardar contra as práticas criminosas, assim buscando evitar a impunidade, práticas vistas para alguns como imprópria, considerando, também, as penas brandas.

Ainda há um extenso percurso a percorrer para alcançar uma legislação que proporcione uma solução verdadeiramente eficaz, que seja capaz de abranger como um todo o uso da internet no Brasil. Embora se tenham leis que tratem os crimes praticados virtualmente, ainda existe uma vulnerabilidade, o Brasil encontra-se ainda muito atrasado no âmbito jurídico sobre o tema se comparado a outros países, e com punições muito branda.

Entretanto, com a adesão do Brasil à Convenção de Budapeste, se espera uma aplicação mais rigorosa das leis que regem o direito digital, essa adesão representa um importante marco para a legislação brasileira, pois o surgimento de uma nova legislação aprimorada é necessário a fim de reduzir a ocorrência de crimes cibernéticos, assegurando simultaneamente a segurança digital e a proteção do direito penal brasileiro, trazendo uma organização mais precisa e direcionada a prevenção, tipificação e combate dos crimes digitais, uma legislação pensada para se adequando a constante evolução das redes de comunicação, assim visando evitar a criação de novas lacunas, impedindo a impunidade dos agentes de delitos virtuais.

REFERÊNCIAS

AZEREDO, Caroline M. de Oliveira, DE CARLOS, Paula Pinhal, WENDET, Emerson. **A internet e a violência contra a mulher:** uma análise sobe a aplicação da Lei Maria da Penha aos casos de violência psicológica no contexto virtual. Revista dos Tribunais. Vol. 119/2016, 2016. Disponível em: http://bdjur.stj.jus.br/jspui/handle/2011/100825. Acesso em: 20 Out. 2023.

BARRETO, Erick Teixeira. **Crimes cibernéticos sob a égide da Lei n. 12.737/2012**, março 2017. Disponível em: http://www.conteudojuridico.com.br/consulta/artigos/49678/crimesciberneticos-soba-egide-da-lei-12-737-2012. Acesso em: 10 set. 2023.

BARRETO, Alessandro Gonçalves; **Vingança Digital:** Compartilhamento não autorizado de conteúdo íntimo na internet, procedimentos de exclusão e investigação policial. Rio de Janeiro. 1ª ed. Mallet Editora. 2017.

BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. **Diário Oficial da União**, Brasília, DF, 07 dec. 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 18 ago. 2023.

BRASIL. Lei n° 12.737, de 30 de novembro de 2012. Lei dos Crimes Digitais. **Diário Oficial da União**, Brasília, DF, 30 dec. 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 17 ago. 2023.

BRASIL. Lei n° 12.965, de 23 de abril de 2014. Marco Civil da Internet. **Diário Oficial da União**, Brasília, DF, 30 dec. 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 28 ago. 2023.

BRASIL. Lei n° 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. **Diário Oficial da União**, Brasília, DF, 15 ago. 2018. Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 11 abr. 2023.

BRASIL. Decreto n° 11.491, de 13 de abril de 2023. Convenção sobre o Crime Cibernético. **Diário Oficial da União**, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm. Acesso em: 14 nov. 2023.

CAPEZ, Fernando Prado. **Código Penal Comentado**. São Paulo: Saraiva, 2016.

CARVALHO, Maria Augusta. **Marco Civil brasileiro para a Internet já é copiado no exterior**, ConJur, 2 set. 2014. Disponível em: <https://www.conjur.com.br/2014-set-02/marco-civil-brasileiro-internet-copiado-exterior>. Acesso em: 10 set. 2023.

CASTELLS, Manuel. **A galáxia da internet**: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar, 2003

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011.

CUNHA, Rogério Sanches; PINTO, Ronaldo Batista. **Violência Doméstica**: Lei Maria da Penha Comentada Artigo por Artigo. São Paulo: Revista dos Tribunais, 2015.

FERREIRA, Guto. **Segurança cibernética**: ameaças e desafios, 19 Jul. 2019. Disponível em: https://www.abdi.com.br/postagem/seguranca-ciberneticaameacas-e-desafios. Acesso em 10 out. 2023.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. **17º Anuário Brasileiro de Segurança Pública**. São Paulo: Fórum Brasileiro de Segurança Pública, 2023. Disponível em: forumseguranca.org.br/wp-content/uploads/2023/07/anuario-2023.pdf. Acesso em: 29 set. 2023

ISAACSON, Walter. **Os inovadores.** São Paulo: Campanhia das letras, 2014.

JESUS, Damásio de; MILAGRE, José Antônio. **Manual de Crimes Informáticos**. São Paulo: Saraiva, 2016.

PANNAIN, Camila Nunes; PEZZELLA, Maria Cristina. **Liberdade de Expressão e Hate Speech na Sociedade da Informação**. Revista Direitos Emergentes da Sociedade Global, Santa Maria, 2015. Disponível em: https://doi.org/10.5902/2316305419432 . Acesso em: 09 Out. 2023.

PINHEIRO, Patrícia Peck. **Direito digital**. 7. Ed. São Paulo: Saraiva, 2021.

RECUPERO, P. R. **New Technologies, New Problems, New Laws**. The Journal of the American Academy of Psychiatry and the Law, Bloomfield, v. 44, n. 3, set. 2016.

ROSSINI, Augusto. **Informática, Telemática e Direito Penal**. São Paulo: Memória Jurídica Editora, 2004.

SILVA, L. W. **A internet foi criada em 1969 com o nome de "Arpanet" nos EUA**. Folha de S.Paulo, 18 ago. 2001. Disponível em:https://www1.folha.uol.com.br/folha/cotidiano/ult95u34809.shtml. Acesso em: 17 set. 2023.

SILVA, Aurélia Carla Queiroga; BEZERRA, Margaret Darling; SANTOS, Wallaz Tomaz. **Relações Jurídicas Virtuais:** Análise de Crimes Cometidos com o Uso da Internet. Revista Cesumar Ciências Humanas e Sociais Aplicadas, v.21, n.1, jan./jun. 2016. Disponível em: https://periodicos.unicesumar.edu.br/index.php/revcesumar/article/view/3952. Acesso em: 24 set. 2023.

SOUZA, Henry Leones; VOLPE, Luiz Fernando Cassilhas. **Da ausência de legislação específica para os crimes virtuais**. 19 Jul. 2015. Disponível: https://egov.ufsc.br/portal/conteudo/da-aus%C3%AAncia-de-legisla%C3%A7%C3%A3o-espec%C3%ADfica-para-os-crimes-virtuais. Acesso em: 19 set. 2023.

STOCO, Isabela Maria; BACH, Marion. **A Mulher como vítima de crimes virtuais**: Legislação e a Jurisprudência. Caderno PAIC, 19(1), 679–698. 14 Nov. 2018.

Disponível em: https://cadernopaic.fae.edu/cadernopaic/article/view/311. Acesso em: 19 set. 2023.

SYDOW, Spencer Toth. **Delitos informáticos próprios**: uma abordagem sob a perspectiva vitimodogmática. 2009. Dissertação (Mestrado em Direito Penal) - Faculdade de Direito - Universidade de São Paulo, São Paulo, 2009. Disponível em: https://doi.org/10.11606/D.2.2009.tde-15062011-161113 . Acesso em: 17 Out. 2023.

VIEIRA, Eduardo. **Os bastidores da Internet no Brasil** – Editora Manole Ltda., 2003.

VILHA, Ana Patrícia Morales; **E-Marketing para bens de consumo durável**. Rio de Janeiro. Editora FGV. 2002.

ANEXO I - DECLARAÇÃO DE CORREÇÃO ORTOGRÁFICA

FACULDADE
ViaSapiens
A IDENTIDADE DO CONHECIMENTO

DECLARAÇÃO DE CORREÇÃO GRAMATICAL

DECLARO para os devidos fins, que realizei a correção gramatical do Trabalho de Conclusão de Curso de Graduação em Direito intitulado: Cibercriminalidade: Análise da evolução da legislação brasileira sobre crimes virtuais, realizado pela acadêmica: Carla Evelyn Silva Souza , da Faculdade Via Sapiens – FVS.

Por ser verdade, firmo a presente.

Tianguá, 28 de novembro de 2022.

Wagner Bento da Silva

Professor: Wagner Bento da Silva

Graduado em: Letras com habilitação em linguas Portuguesa e Inglesa

Especialista em: Gestão Escolar

Portador do registro profissional nº 117,livro GS-13, folha 57, proc. 00918/09