CRIMES CIBERNÉTICOS: O QUE SÃO, QUAL SEU REAL PERIGO E A IMPORTÂNCIA DE DISPOSITIVOS QUE GARANTAM A SEGURANÇA DA SOCIEDADE[1]

Carlos Henrique Machado Borges[2]

Yasmyn Cardoso Quinan[3]

Maressa de Melo Santos[4]

RESUMO

A pesquisa parte da hipótese de que a legislação, apesar de ter avançado muito nos últimos anos, criando novos dispositivos e se atentando à rápida expansão do mundo virtual, ainda não consegue prevenir e proteger a sociedade de todos os perigos provenientes do ambiente virtual. Fomentando a discussão a respeito das leis 12.737/12 e 12.965/14 e mostrando como a jurisdição brasileira se comporta a respeito dos crimes cibernéticos, busca-se explicitar de forma concisa os principais pontos das leis trabalhadas e mostrar a importância de dispositivos jurídicos que visam a proteção dos direitos do indivíduo em âmbito virtual. Mostraremos o que aduzem Emerson Wendt e Higor Vinicius Nogueira Jorge, sobre os crimes cibernéticos. Também será mostrado o andamento da democracia digital pela ótica de Wilson Gomes, que é o referencial teórico, das teorias da sociedade e exceção. Outro ponto de relevância é citar, explicar e exemplificar de que forma agem aqueles que praticam condutas virtuais tipificadas no Código Penal, como são esses crimes cibernéticos. Além disso, em qual estado se encontram os crimes cibernéticos na atual sociedade e qual a projeção dos mesmos para os próximos anos, tendo por base uma perspectiva crítica do crime segundo Zaffaroni.

Palavras-chave: sociedade e criminologia midiática; Lei Carolina Dieckman; marco civil da internet; metaverso

ABSTRACT

The research is based on the hypothesis that legislation, despite having advanced a lot in recent years, creating new devices and paying attention to the rapid expansion of the virtual world, is still unable to prevent and protect society from all dangers arising from the virtual environment. Promoting discussion regarding laws 12,737/12 and 12,965/14 and showing how Brazilian jurisdiction behaves regarding cybercrimes, we seek to concisely explain the main points of the laws worked on and

---

[1] Trabalho de Conclusão de Curso apresentado à Faculdade de Inhumas FacMais, como requisito parcial para a obtenção do título de Bacharel em Direito, no segundo semestre de 2023.

[2] Acadêmico Carlos Henrique Machado Borges do 10º Período do curso de Direito pela Faculdade de Inhumas. E-mail: carlos@aluno.facmais.edu.br

[3] Acadêmica Yasmyn Cardoso Quinan do 10º Período do curso de Direito pela Faculdade de Inhumas. E-mail: yasmyn@aluno.facmais.edu.br

[4] Professor(a)-Orientador(a). Especialista em Direito Internacional. Docente da Faculdade de Inhumas.E-mail: maressa@facmais.edu.br

show the importance of legal provisions that aim to the protection of individual rights in a virtual environment. We will show what Emerson Wendt and Higor Vinicius Nogueira Jorge say about cybercrimes. The progress of digital democracy will also be shown from the perspective of Wilson Gomes, who is the theoretical reference for theories of society and exception. Another point of relevance is to mention, explain and exemplify how those who practice virtual conduct typified in the Penal Code act, such as these cyber crimes. Furthermore, what state are cybercrimes in today's society and what is their projection for the coming years, based on a critical perspective of crime according to Zaffaroni.

Keywords: cybercrimes, society and media criminology, Law Carolina Dieckman, internet civil milestone, metaverse

1 INTRODUÇÃO

A presente pesquisa tem como objetivo estudar e analisar a evolução das leis referentes aos crimes cibernéticos, a evolução destes crimes, e o que ainda há de se melhorar nos estudos que tange à temática.

A explosão da internet, que surgiu no fim dos anos 90 e início dos anos 2000, e a cada dia mais tem sido usada, faz com que as pessoas convivam menos umas com as abrindo brechas para pessoas mal intencionadas cometerem crimes cibernéticos.

Este artigo irá abordar os crimes cibernéticos com ênfase na Lei nº 12.737/12, e também dará enfoque a Lei nº 12.965/14, conhecida como “Marco Civil da Internet”. Ele também trará uma perspectiva da teoria da criminologia midiática de Zaffaroni.

O objetivo precípuo é problematizar o lugar da positivação das leis penais virtuais dentro da ciência penal digital, com uma perspectiva crítica.

O estudo foi fundamentado com literatura de Túlio Vianna e Felipe Machado, além dos escritos de Emerson Wendt e Higor Vinicius Nogueira Jorge, autores que ajudaram a fundamentar os “Crimes Cibernéticos”. No âmbito penal trarei o autor de Direito Penal, Cleber Masson, que nos auxiliará mais na questão legislativa, e também Eugenio Raúl Zaffaroni que trata a respeito da teoria da criminologia midiática.

A parte da hipótese de que a legislação, apesar de ter avançado muito nos últimos anos, criando novos dispositivos e se atentando à rápida expansão do mundo virtual, ainda não consegue prevenir e proteger a sociedade de todos os perigos que a internet pode oferecer.

Para tanto, a metodologia utilizada será a realização de pesquisa bibliográfica e estudo teórico sobre a temática Crimes Cibernéticos, para que possa ter um referencial teórico a respeito do tema, podendo assim saber as dificuldades de lidar com eles.

2 COMPUTADORES E INTERNET

Nesta parte objetiva analisar a forma como a tecnologia mudou a sociedade atual. Será abordada a relação dos computadores e a internet.

2.1 Os computadores e a internet

Os primeiros computadores da era moderna surgiram na década de 40, enormes máquinas que ocupavam andares inteiros de prédios e utilizavam quilômetros de fios. Como é dito por Pinheiro (2013):

> A utilização de máquinas calculadoras mecânicas e eletromecânicas proliferou no início do século XX. Nos anos 30, essas máquinas começaram a ser construídas com relés eletromagnéticos, porém somente em 1946 estaria finalizado o engenho que claramente se reputaria um passo além das calculadoras. Seu nome era ENIAC — Eletric Numeric Integrator and Calculator —, um computador baseado em circuitos eletrônicos. Operava com lógica binária, composto de 18.000 válvulas, e ocupava diversas salas da Universidade de Pensilvânia, onde foi concebido. (Pinheiro, 2013, p. 32).

Os computadores dessa época sofriam com superaquecimento devido às altas temperaturas que a máquina atingia. Com o tempo as máquinas foram se aperfeiçoando e ficando cada vez mais rápidas. Esse desenvolvimento não cessou, e até os dias de hoje como se pode perceber a velocidade e capacidade de memória dos computadores está cada vez maior, e seu tamanho cada vez menor, como por exemplo os smartphones, que são altamente consumidos pela sociedade contemporânea.

Já a internet é um sistema global de redes de computadores interligadas que utilizam protocolos para servir gradativamente para todos os usuários. Esse sistema foi criado, a princípio, com intuito militar no início da década de 60, sendo liberado para utilização comercial apenas no início da década de 1990. Como aduz Jorge e Wendt (2013)

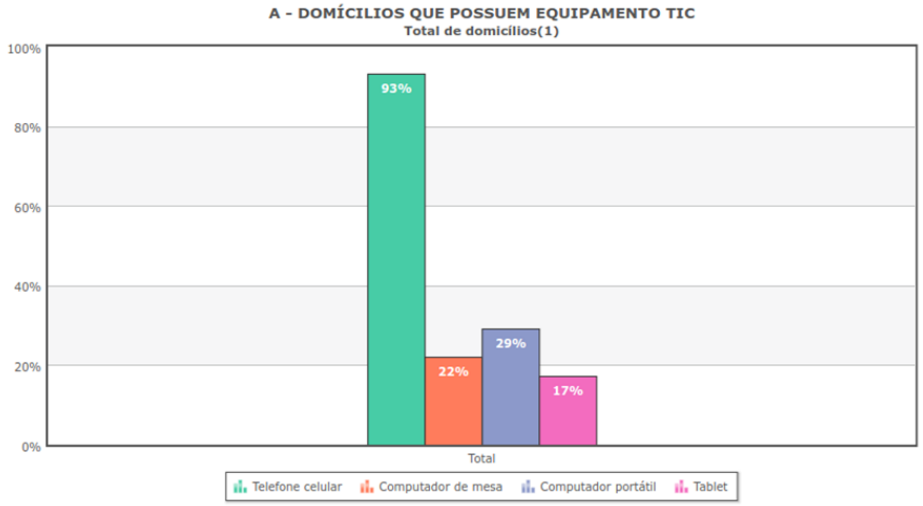
> No ano seguinte (1962) a Força Aérea, com a preocupação de proteger-se de uma eventual guerra ou ataque nuclear, solicitou à empresa Rand Corporation um estudo sobre uma rede de comunicação militar descentralizada, ou seja, despida de um núcleo central, que funcionasse mesmo que fossem destruídos alguns de seus terminais (Jorge; Wendt, 2013, p. 06).

Após isso tomou conta da vida da maioria dos indivíduos da sociedade, uma vez que atualmente as pessoas fazem compras pela internet, encontram relacionamentos, trabalham e estudam, ou seja, a vida no mundo real foi gradativamente sendo transferida para a internet. E essa transferência vem sendo contínua e sem previsão de redução, pois a internet encurta as distâncias, economiza o tempo, algo que hoje na sociedade ativa e apressada em que vivemos, se torna de imprescindível, e também é algo prático, se tem acesso a internet de qualquer lugar, independente do horário ou tempo ela está lá para ser utilizada.

Sendo assim, a tendência é que cada vez mais a Internet tome conta da vida da sociedade, tornando-se indispensável, assim como a energia elétrica está presente nos dias atuais.

Em uma pesquisa realizada em 2018 pela CETIC, foi demonstrado que 93% das pessoas entrevistadas tinham acesso à internet pelo celular, que hoje é o meio mais fácil de conectar-se a internet.

Gráfico 1 - Domicílios que possuem equipamentos TIC



Fonte: *CGI.br/NIC.br, Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br)*

Outro item que podemos observar é que o computador de mesa a cada dia perde mais espaço para os portáteis, principalmente pela facilidade de locomoção, e isso não só pelos telefones, mas também pelos notebooks e tablets que na atualidade estão tendo sendo atualizado com o mesmo objetivo de uso que os computadores.

Na atualidade a cada dia estudam para renovação nas tecnologias para mais conforto e facilidade na vida de estudantes e profissionais, deixando tudo de difícil para trás e mantendo apenas os mais tecnológicos e facilitados.

3 LEIS CIBERNÉTICAS

Será feito uma análise das leis cibernéticas, que surgiram em 2012 com a Lei Carolina Dieckmann, seguida pelo Marco Civil da Internet em 2014, já em 2018 surgiu a Lei Geral de Proteção de Dados e por último a Emenda Constitucional 115 que garante a proteção de dados pessoais, e assim as leis cibernéticas só tendem a aumentar, como será visto a seguir.

3.1 Lei Carolina Dieckmann (Lei 12.737/12)

A lei traz o acréscimo de dois artigos ao Código Penal, os artigos 154-A e o 154-B. o artigo 154-A tipifica que:

> 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 (Brasil, 2012).

Esse dispositivo tipifica que invadir o aparelho de terceiros, como por exemplo o smartphone, torna-se crime, algo que antes não era tipificado em código algum,

fazendo com que a legislação brasileira, que era falha nesse aspecto conseguisse suprir a falta de uma norma específica para esse tipo de ato delituoso.

Já o artigo 154-B apenas complementa o primeiro, trazendo que os crimes só procedem mediante a representação, exceto em casos que o crime é praticado contra a ordem pública. A lei também altera o artigo 266 do Código Penal, incluindo os dispositivos informáticos no âmbito dos dispositivos abrangidos pelo mesmo. Outra alteração é a inclusão do cartão de crédito como documento particular, que está tipificado no artigo 298 do Código Penal, com isso a lei que pune falsificação de documento particular também englobou os cartões de créditos, dando margem para que aqueles que praticam esse ato inflacionário via dispositivo informático possa ser também punido com o devido rigor.

Essas medidas trouxeram para o ordenamento jurídico brasileiro uma proteção e sigilo dos dados dos indivíduos na rede mundial de computadores, demonstrando a atenção que os legisladores têm tido quanto à modernização do Código Penal, dado que a tendência é de que o mesmo tem que tender a acompanhar a modernização da sociedade. Dessa forma, podemos entender que a tipificação de crimes em ambiente virtual é um passo importante para esse acompanhamento.

Na atualidade, cada vez mais pessoas necessitam de seus aparelhos eletrônicos, seja para trabalho, estudo ou lazer. Assim é necessário oferecer a esses indivíduos uma segurança maior no ambiente virtual, visto que cada vez mais as pessoas acessam suas contas bancárias, colocam seus dados pessoais em cadastros, entre outras situações cotidianas. E por isso se fez necessário que surgisse uma lei como a Lei nº 12.737/12 que zelasse pela segurança dos indivíduos, e por seu direito à privacidade, que já é garantido pela Constituição Federal de 1988. A respeito disso Peck (2013) declara:

> Com as mudanças ocorridas desde então, ingressamos na era do tempo real, do deslocamento virtual dos negócios, da quebra de paradigmas. Essa nova era traz transformações em vários segmentos da sociedade — não apenas transformações tecnológicas, mas mudanças de conceitos, métodos de trabalho e estruturas. O Direito também é influenciado por essa nova realidade. A dinâmica da era da informação exige uma mudança mais profunda na própria forma como o Direito é exercido e pensado em sua prática cotidiana (Peck, 2013, p.26)

Logo, é possível entender o impacto e a importância dessa lei no que se refere a crimes cibernéticos, isto é, ela significa a evolução da proteção ao cidadão no que tange à esse tipo de crime. Contudo, é importante ressaltar que ainda deixa muito a desejar nesse âmbito, mas que tenta, no que diz respeito à defesa do usuário da rede mundial de computadores, trazer algo de novo e não permanecer tão aquém da evolução que o uso de aparelhos informáticos traz a atual realidade.

3.2 Marco civil da internet (Lei 12.965/14)

A Lei nº 12.965/14, mais conhecida como Marco Civil da Internet foi sancionada pela então presidente Dilma Rousseff, no ano de 2014, e veio para servir como um guia de comportamento na internet. Isto é, essa lei foi responsável por estabelecer princípios, normas e garantias no que diz respeito ao convívio dos indivíduos na internet, tendo como principal objetivo prever e tipificar as práticas criminosas no ambiente virtual, além de defender as liberdades de todos na internet. Pode-se perceber então que essa Lei foi além do que qualquer lei jamais foi, no que

diz respeito ao uso rede mundial de computadores, pois além de tipificar os crimes oriundos da utilização da internet, também garante os direitos daqueles que utilizam a rede.

Outro ponto importante do marco civil é a defesa da privacidade dos usuários, defendendo assim um dos direitos basilares previstos pela Constituição Federal, fazendo valer o direito de todos de terem sua privacidade resguardada. Muitos acreditaram que o Marco Civil viria para limitar as liberdades dos usuários, porém ela percorreu o caminho contrário, tentando garantir que essas liberdades não fossem enfraquecidas ou desrespeitadas. Segundo o site Techtudo, em uma pesquisa feita em janeiro de 2022 constatou que o brasileiro teria passado 91 horas online por semana, ou seja, mais da metade do dia, é necessário que haja legislações específicas que defendam os direitos dos mesmos.

Além disso, o Marco Civil traz a neutralidade de rede que consiste na democratização da qualidade da internet que é oferecida para os usuários, sem que haja qualquer tipo de limite, censura ou boicote dos conteúdos que na internet estão disponíveis, sendo assim um dispositivo que preza pela liberdade de informação dos usuários, algo que não é garantido em muitos países do mundo que vivem à mercê daquilo que o governo oferece como verdade.

No caso da Lei em questão o bem tutelado é a inviolabilidade dos dados informáticos. Como é dito por Vianna, Machado (2013):

> O bem jurídico penalmente tutelado é a inviolabilidade dos dados informáticos, corolário do direito a privacidade e intimidade presentes na Constituição da República, em seu art. 5º, X. A inviolabilidade compreende não só o direito à privacidade e ao sigilo dos dados, como também à integridade destes e sua proteção contra qualquer destruição ou mesmo alteração (Vianna; Machado, 2013, p. 94).

Outro trecho que ressalta esse importante instituto é o artigo 4° da referida lei, que ressalta o compromisso com a liberdade de expressão, o direito de acesso à internet por todos, do acesso à informação, ao conhecimento e a participação à vida cultural, entre outros.

O marco civil se mostra de grande valia para todos, protegendo e garantindo os direitos que já são garantidos no mundo físico, dentro do mundo virtual, transformando-o em um ambiente muito mais democrático e catalisador de transformações sociais, e também tipificando, punindo, e prevenindo os possíveis crimes que poderiam vir a ocorrer em ambiente cibernético. Mais uma vez mostrando que o legislador brasileiro está atento às mudanças que ocorrem na realidade social do Brasil, e que é necessário acompanhar a modernização da sociedade, sempre respeitando seus direitos e protegendo seus valores basilares.

3.3 Lei Geral de Proteção de Dados (LGPD) (Lei 13.709/18)

A Lei Geral de Proteção de Dados pessoais ela foi criada com o intuito é o principal fundamento de proteger os direitos de liberdade e privacidade, e também com o objetivo de criar uma segurança jurídica com padrões de regulamentos e práticas para proteger os dados pessoais de todo cidadão que esteja no Brasil, para que isso funcione a lei trouxe alguns tipos de conceitos, objetivos, princípios e regras para que possa se tornar válida, mas a LGPD na sua criação ela se tornou complexa e extensa, tendo a necessidade de estudar para maior compreensão.

De acordo com o artigo 11, II, da lei o consentimento do titular dos dados é considerado elemento essencial para o tratamento. A lei traz como garantia para o cidadão o direito de transferir dados para outro fornecedor de serviços, mas deve ser levado em conta os requisitos de finalidade e necessidade informados ao titular.

O Brasil conta com a instituição ANPD (Autoridade Nacional de Proteção de dados Pessoais) responsável por regular e orientar sobre como aplicar a lei, por esse motivo existem algumas funções nas organizações como o controlador, o operador, e o encarregado.

A LGPD foi sancionada em 2018 e entrou em vigor em 2020, esta lei veio para regulamentar a transmissão de dados pessoais, desde então as empresas tentam regular com a lei e assim não serem penalizados por algum vazamento de dados pessoais, coisa que antes era uma prática comum entre as empresas era a comercialização de dados pessoais, com essa regulamentação essa prática vem diminuindo, como aduz (Souza, Acha)

> Sendo assim, a LGPD, que entrou em vigor em agosto de 2020, contribuiu para dar mais transparência ao tratamento de nossos dados pessoais possibilitando aos cidadãos, em geral, e aos consumidores, em particular, um maior controle sobre suas informações, e cobra das empresas medidas de segurança eficazes para evitar vazamentos (Souza; Acha, 2022, p. 07).

Muitas empresas estão contratando profissionais que já se especializaram em LGPD, para que deem cursos e adequem a empresa para que estas se ajustem à lei.

3.4 Emenda Constitucional Nº 115/2022

Com essa emenda constitucional transformaram a Proteção de Dados Pessoais como uma garantia fundamental, adicionando o inciso LXXIX no Art. 5º da Constituição Federal, como pode-se ver

> LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.
> § 1º As normas definidoras dos direitos e garantias fundamentais têm aplicação imediata.
> § 2º Os direitos e garantias expressos nesta Constituição não excluem outros decorrentes do regime e dos princípios por ela adotados, ou dos tratados internacionais em que a República Federativa do Brasil seja parte.
> § 3º Os tratados e convenções internacionais sobre direitos humanos que forem aprovados, em cada Casa do Congresso Nacional, em dois turnos, por três quintos dos votos dos respectivos membros, serão equivalentes às emendas constitucionais.
> § 4º O Brasil se submete à jurisdição de Tribunal Penal Internacional a cuja criação tenha manifestado adesão.

Com isso a proteção de dados pessoais ganhou ainda mais garantias, já que a Constituição Federal deve ser respeitada acima de todos os outros dispositivos legais. Além disso, também fixou a competência da União para legislar, organizar e fiscalizar a proteção e o tratamento dos dados pessoais.

4 CRIMES CIBERNÉTICOS

Esta parte objetiva analisar os crimes cibernéticos. Para tal ele foi dividido em 03 partes, na primeira parte será abordado os crimes cibernéticos, na segunda os criminosos e as classificações dos crimes e também a mediatização dos crimes cibernéticos.

4.1 Os crimes cibernéticos

Podemos ver que os crimes cibernéticos estão presentes na realidade da nossa sociedade, e que não são algo recente. Segundo Patricia Peck (2013), já existem guerras cibernéticas sendo travadas entre as maiores potências mundiais, uma vez que a espionagem passou a ser cibernética, e muitos outros tipos de rivalidades entre países que antes eram alimentadas pela presença física, agora recorrem ao meio virtual. Essas ações cibernéticas vem maturando juntamente com o ambiente virtual, à medida que expandindo, os crimes cibernéticos também se expandem e tomam novas formas e novas proporções, inclusive com a pandemia acelerou ainda mais esse processo.

Os usuários, mesmo com as mais modernas ferramentas de proteção, estarão sempre expostos ao que está na internet. É bom salientar que não existe hoje ferramenta que proteja de forma 100% eficaz o usuário de um malfeitor, por isso a quantidade de infratores de crimes virtuais só aumenta. Diversos exemplos de casos de empresas que tiveram seus dados vasados, e milhares de clientes expostos, ou mesmo o caso da atriz Carolina Dieckmann que teve fotos pessoais jogadas na rede e sua intimidade exposta. esses casos mostram a real necessidade de leis como a “Lei Carolina Dieckmann” e o “Marco Civil da Internet” que visam proteger e garantir ao usuário as mesmas garantias que ele tem no mundo físico, pois o mundo exterior cada vez mais perde espaço para o mundo virtual, e a não regulação do modo de agir no mundo virtual pode causar problemas gravíssimos em um futuro não tão distante.

Pode-se estar sujeito a crimes cibernéticos a qualquer momento, visto que carregamos o mundo virtual na palma das mãos, no bolso, dentro da mochila, e não precisamos estar necessariamente conectados à internet para que soframos com as mazelas do meio virtual. Podemos ser vítimas de, cyberbullying[5], cyberstalking[6], termos fotos “vazadas” na rede, termos nossos equipamentos invadidos por terceiros, além de outros diversos outros crimes como a pedofilia, a venda online de produtos ilícitos como drogas, armas, explosivos, dentre outros que são proibidos em nosso país.

As infrações cometidas no meio virtual muitas vezes se dão com o auxílio de programas específicos, que auxiliam na atitude ilícita do infrator. Esses softwares são popularmente conhecidos como Vírus. Os Vírus são softwares maliciosos feitos com o intuito de danificar o equipamento, ou roubar dados pessoais do usuário, muito utilizado na espionagem industrial, na espionagem entre países e contra pessoas de classe social elevada, ou que exerçam uma função de suma importância no governo.

---

[5] Cyberbullying: Consiste na utilização do cyber espaço para hostilizar ou intimidar uma pessoa.

[6] Cyberstalking: Consiste na perseguição constante através da internet, os indivíduos que realizam essa perseguição são conhecidos como “Stakers”

O tipo de vírus mais famoso e antigo é o trojan[7] (ou comumente conhecido como cavalo de tróia). Ele abre uma passagem no computador do alvo para que o hacker (ou cracker) possa invadir e fazer o que quiser no computador "infectado".Outro tipo de vírus que causa grandes transtornos é o worm[8], que se difere dos demais vírus por se replicar e infectar outros computadores. Existem casos de centenas de computadores infectados por um único worms. Outro exemplo de vírus popular é o hijacker (também conhecido com spyware), popularmente utilizado pelos hackers para infectar os navegadores como Google Chrome, Mozila e Spark, o objetivo do hijacker é redirecionar o alvo para uma determinada página, e é nesta página que onde se dará o crime. E por último, dentre os mais comuns está o keylogger, uma espécie de vírus que manda para o usuário tudo que a vítima digita em seu computador, ou smartphone, fazendo com que os keyloggers sejam muito utilizados para roubo de senhas.

Em uma analogia com crime de homicídio Vianna e Machado (2013) aduz que

> Em uma analogia com o crime de homicídio, poder-se-ia afirmar que a digitação do comando ou o clicar do mouse equivalem ao disparo de uma arma e a leitura, escrita ou processamento dos dados equivalem à morte da vítima. Assim como matar equivale semanticamente a produzir lesões corporais em outrem, causando-lhe o resultado morte, acessar significa emitir comandos a um sistema computacional, causando a leitura, a escrita ou o processamento de dados. (Vianna; Machado, 2013, p. 57)

Mas nem só de vírus e hackers vivem os crimes cibernéticos Infelizmente vem crescendo em níveis alarmantes a prática de estelionato utilizando-se dos meios virtuais. Essa prática já era utilizada há um bom tempo na internet, e também por meio de ligações, porém com a febre dos aplicativos de mensagens instantâneas esse número cresceu de forma assustadora, transformando esse crime em algo preocupante, tanto para a sociedade quanto para o Direito.

Engana-se quem pensa que os crimes cibernéticos se restringem somente a uma única camada social. Vale ressaltar que as pessoas jurídicas também podem ser alvo e autor de crimes cibernéticos. Segundo Patricia Peck (2013), um dos crimes mais recorrentes hoje é o da espionagem industrial e com a ajuda da tecnologia esse ato delituoso se espalhou de forma avassaladora pelo mercado empresarial, por isso cada vez mais os empresários buscam maneiras de proteger seus dados e os dados de seus clientes. Existem casos recentes de empresas que sofreram com ataques cibernéticos e tiveram seus dados e ou de seus clientes expostos na rede, isso gera um enorme problema tanto para empresa que havia se comprometido a manter os dados de seus clientes em sigilo, quanto para os clientes que tem dados como números e senhas de cartão, identidade dentre outras informações pessoais vazadas na rede.

Ainda no tocante ao crime de espionagem virtual, outro ponto que poucos sabem é que os países migraram sua espionagem para a rede mundial de computadores. Isso se deve ao fato de que na rede não existem fronteiras, o que torna o trabalho dos espiões mais fácil e seguro, assim sendo os países travam uma real guerra cibernética visando coletar o maior número de informações possível dos

---

[7] Trojan: Habitualmente o cavalo de Tróia chega a simular funções de certa relevância para o usuário, suas ações maliciosas geralmente acontecem em segundo plano, longe das vistas do alvo, é muito utilizado para o robô de documentos, senhas e outros arquivos.

[8] O worm infecta outros aparelhos através de qualquer tipo de conexão, seja ele uma rede local ou pela própria internet.

outros países, visando o conhecimento de seu estado econômico, poderio bélico, entre outras coisas e também se proteger das possíveis espionagens provenientes destes mesmo países.

4.2 Os criminosos e a classificação dos crimes

Os Crackers são, na maioria dos casos, os autores dos crimes cibernéticos. Como é explanado por Ângelo e Sanches (2018):

> Junto aos cybercrimes surgem duas figuras, sendo elas, o hacker e o cracker. Embora a expressão hacker geralmente aparece associada a infrações virtuais, são os crackers os reais criminosos. A diferença entre eles está no modo em como utilizam seus conhecimentos tecnológicos (Angelo; Sanches, 2018)

Essas pessoas se dedicam excessivamente aos softwares de computador, e por sua vez acham brechas que possibilitam a invasão de equipamentos alheios para que e assim possam roubar dados, danificar o equipamento, geralmente visando extorquir a vítima, como no caso da atriz Carolina Dieckmann.

Existem também aqueles que simplesmente desenvolvem formas de tapar as brechas de segurança, geralmente contratados por grandes empresas que visam a melhor proteção de seus dados.

Por muitas vezes os Crackers são confundidos com os Hackers, o que é um ledo enganoso, pois ambos são opostos. Enquanto o cracker visa burlar um sistema em troca de uma vantagem ilícita, na maioria das vezes, o hacker por sua vez nada mais é que um programador com vasta experiência, e que é geralmente contratado por empresas para dar consultorias e oferecer produtos que possam blindar as empresas de possíveis ataques dos crackers. Ou seja, hackers e cracker são basicamente antônimos, enquanto um destrói e rouba o outro trabalha em prol da proteção e manutenção dos sistemas de computadores.

Os crimes cibernéticos podem ser classificados em crimes próprios, que são os crimes cometidos apenas no âmbito virtual.

Aduz Vianna e Machado (2013) que

> Além do crime de invasão de dispositivo informático, há outras condutas que caracterizam delitos que têm como objeto a inviolabilidade dos dados informatizados e, portanto, podem ser classificados como delitos informáticos próprios (Vianna; Machado, 2013, p. 32).

A Lei nº 12.737/12, tipifica esse tipo de crime, e podemos citar como exemplo o ato de pegar uma foto íntima de uma pessoa e disponibilizar para todos na internet. Já os crimes impróprios são aqueles que a internet é apenas uma ferramenta intermediária para o cometimento de crimes. Um exemplo de crime impróprio é a pedofilia com o auxílio da internet, pois o pedófilo utiliza-se da internet para atrair as crianças das mais diversas formas, seja se passando por outra criança, oferecendo recompensas ou até mesmo ganhando a confiança da criança, e no mundo real comete onde comete o ato criminoso.

4.3 Midiatização dos crimes cibernéticos

Os Crimes Cibernéticos, derivam dos chamados “crimes de cifras douradas”, uma vez que, ambos são cometidos por pessoas com um intelecto maior, utilizando

de técnicas para cometer os delitos.Um crime cibernético que ficou comum na pandemia foi o estelionato virtual, onde os infratores utilizam das redes sociais para se passar por um amigo ou familiar e pedem dinheiro emprestado por PIX, por exemplo. Segundo a empresa de cibersegurança PSAFE, de janeiro a novembro de 2021 houve mais de 44 milhões de tentativas de golpes virtuais. Esses crimes estão sempre na mídia, e como Zaffaroni diz, a criminologia midiática sempre existiu, porém com a democratização da internet, teve um grande aumento.

Zaffaroni em seu livro “A questão criminal”, diz que

> A criminologia midiática sempre existiu e sempre apela a uma criação da realidade através de informação, subinformação e desinformação em convergência com preconceitos e crenças, baseada em uma etiologia criminal simplista, assentada na causalidade mágica. Isso sempre aconteceu e o que vimos **René Girard** explica claramente: se o sistema penal tem por função real canalizar a vingança e a violência difusa da sociedade, é mister que as pessoas acreditem que o poder punitivo está neutralizando o causador de todos seus males (Zaffaroni, 2013, p. 132).

Nessa fala de Zaffaroni, e na tese de Girard, esses infratores tornam-se bode expiatórios, que a mídia cria para criminalizar ainda mais os delitos cometidos, as mídias que antes eram apenas o rádio e a televisão, agora também contam com a internet que mostram as notícias em tempo real e mostram meios de minimizar tais delitos.

5 IMPORTÂNCIA DE DISPOSITIVOS QUE GARANTAM A SEGURANÇA DA SOCIEDADE

A importância de dispositivos que garantam a segurança da sociedade contra crimes cibernéticos é crucial na era digital em que vivemos. Esses dispositivos desempenham um papel essencial na proteção de dados, sistemas e infraestrutura crítica contra ameaças cibernéticas.

Patricia Peck (2013), nos fala sobre a questão da segurança cibernética, vejamos

> A questão da segurança é um dos principais temas a serem discutidos e resolvidos não apenas no Direito Digital, mas na sociedade como um todo, uma vez que é uma das barreiras para o maior aproveitamento das novas tecnologias e um limitador para a exploração de seu potencial comercial. Como já vimos, a necessidade de segurança nas expectativas da sociedade foi um dos fatores que motivaram a criação do próprio Direito como fenômeno de controle das condutas, e do Estado como ente autorizado a praticar o controle dentro de limites permitidos pela própria sociedade por meio das leis — o chamado Estado de Direito. Por isso, é lógico imaginar que toda nova tecnologia que possibilite uma nova ferramenta de relacionamento necessite de um estudo mais profundo sobre a sua capacidade em transmitir segurança e ter no Direito um mecanismo que possa garanti-la. (Peck, 2013, p. 77)

Aqui estão alguns pontos que destacam a relevância desses dispositivos:

1. Proteção de Dados Pessoais e Empresariais:
    - Dispositivos de segurança cibernética, como firewalls e antivírus, ajudam a proteger informações pessoais e empresariais sensíveis contra acesso não autorizado e roubo por parte de criminosos cibernéticos.
2. Prevenção de Ataques Cibernéticos:
    - Esses dispositivos desempenham um papel fundamental na prevenção de uma variedade de ataques, incluindo malware, ransomware e phishing, que podem ter impactos devastadores em indivíduos, empresas e até mesmo em infraestruturas críticas.
3. Manutenção da Integridade de Sistemas:
    - Mecanismos de detecção de intrusões e sistemas de prevenção ajudam a manter a integridade dos sistemas, evitando alterações não autorizadas e garantindo que os sistemas operem conforme projetado.
4. Segurança Financeira e Econômica:
    - Crimes cibernéticos podem resultar em perdas financeiras significativas para empresas e indivíduos. Dispositivos de segurança desempenham um papel crucial na proteção contra fraudes financeiras, roubo de identidade e outros ataques que impactam a estabilidade econômica.
5. Garantia da Continuidade dos Negócios:
    - Empresas dependem cada vez mais da tecnologia para operar. Dispositivos de segurança contribuem para garantir a continuidade dos negócios, protegendo contra interrupções causadas por ataques cibernéticos.
6. Proteção de Infraestrutura Crítica:
    - Setores críticos, como energia, transporte e saúde, dependem fortemente de sistemas digitais. A segurança dessas infraestruturas é vital para a segurança nacional.
7. Preservação da Privacidade Online:
    - Dispositivos de segurança auxiliam na preservação da privacidade online, protegendo contra monitoramento não autorizado e coleta indevida de dados.
8. Confiança na Tecnologia:
    - A confiança na tecnologia é essencial para a adoção generalizada. Dispositivos de segurança contribuem para a construção dessa confiança, assegurando que os usuários se sintam seguros ao utilizar serviços online e realizar transações.
9. Enfrentamento de Ameaças Emergentes:
    - Com o surgimento constante de novas ameaças cibernéticas, dispositivos de segurança desempenham um papel adaptativo, ajudando a enfrentar e mitigar ameaças emergentes por meio de atualizações e tecnologias avançadas.
10. Proteção contra Ataques de Estado e Grupos Organizados:
    - Dispositivos de segurança desempenham um papel fundamental na defesa contra ataques cibernéticos patrocinados por estados e grupos organizados, que podem visar a infraestrutura crítica e a segurança nacional.

A combinação de conscientização, educação, práticas de segurança sólidas e o uso contínuo e eficaz de dispositivos de segurança cibernética é essencial para enfrentar os desafios em constante evolução no cenário de ameaças cibernéticas.

6 CONSIDERAÇÕES FINAIS

O artigo oferece uma análise profunda sobre a evolução das leis relacionadas aos crimes cibernéticos, destacando a importância crescente dos dispositivos de

segurança na sociedade digital. A evolução legislativa, evidenciada por marcos como a Lei Carolina Dieckmann, o Marco Civil da Internet, a LGPD e a Emenda Constitucional nº 115/2022, reflete uma preocupação em adaptar as normas à rápida transformação tecnológica e aos novos desafios trazidos pelos crimes online.

Neste contexto, a proteção jurídica se torna crucial na era digital, considerando a sociedade cada vez mais dependente da tecnologia. Apesar dos avanços legislativos, o texto aponta para desafios persistentes na prevenção e proteção contra os perigos que a internet pode oferecer, destacando a necessidade contínua de adaptação das leis para enfrentar ameaças emergentes.

A seção que aborda a evolução tecnológica, desde os primeiros computadores até os dispositivos portáteis modernos, destaca a relevância da internet em diversas esferas da vida cotidiana, como compras, relacionamentos, trabalho e estudo. A análise ressalta como a tecnologia moldou profundamente a sociedade e, consequentemente, a legislação que busca regulamentar esse cenário em constante transformação.

O texto destaca, ainda, a importância das leis cibernéticas, como a Lei Carolina Dieckmann, o Marco Civil da Internet, a LGPD e a Emenda Constitucional, na garantia de direitos fundamentais na era digital, especialmente no que diz respeito à privacidade e proteção de dados pessoais. Essas normativas visam estabelecer princípios, normas e garantias para um convívio online seguro e respeitoso.

A seção dedicada aos crimes cibernéticos oferece uma visão abrangente, abordando desde vírus e hackers até crimes próprios e impróprios. Destaca-se a importância de compreender a diversidade de ameaças virtuais, incluindo estelionato virtual, espionagem industrial e a crescente problemática do cibercrime na sociedade contemporânea.

A análise da midiatização dos crimes cibernéticos destaca como a mídia influencia a percepção pública desses delitos, evidenciando a criminologia midiática. A internet, embora tenha democratizado a informação, também contribuiu para a criação de bodes expiatórios na sociedade, moldando a forma como os crimes cibernéticos são percebidos e discutidos.

A seção final sublinha a crucial importância dos dispositivos de segurança cibernética na proteção da sociedade. Esses dispositivos desempenham papéis fundamentais na proteção de dados, prevenção de ataques e manutenção da integridade dos sistemas, ressaltando a necessidade contínua de investimento em tecnologias que fortaleçam a cibersegurança.

Em síntese, o trabalho oferece uma visão abrangente e atualizada sobre o panorama dos crimes cibernéticos, as leis que buscam regulamentar esse cenário, a evolução tecnológica e a importância dos dispositivos de segurança na sociedade digital, destacando a complexidade e a necessidade de adaptação constante nesse contexto em constante evolução.

REFERÊNCIAS

BORGES, Abimael. Lei Carolina Dieckmann - Lei nº. 12.737/12, art. 154-a do Código Penal. Disponível em: https://abimaelborges.jusbrasil.com.br/artigos/111823710/lei-carolina-dieckmann-lei-n-12737-12-art-154-a-do-codigo-penal. Acesso em: 14 jun. 2022

BRASIL. LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm. Acesso em: 14 jun. 2022.

BRASIL. LEI Nº 12.965, DE 23 DE ABRIL DE 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 14 jun. 2022.

MASSON, Cleber. Código Penal comentado. 2. ed. rev., atual. e ampl. - Rio de Janeiro: Forense; São Paulo: MÉTODO, 2014.

PINHEIRO, Patricia Peck. Direito digital / Patricia Peck Pinheiro. — 5. ed. Rrev., atual. e ampl. de acordo com as Leis n. 12.735 e 12.737,de 2012 — São Paulo: Saraiva, 2013

SANCHES, Ademir Gasques; ANGELO, Ana Elisa. **INSUFICIÊNCIA DAS LEIS EM RELAÇÃO AOS CRIMES CIBERNÉTICOS NO BRASIL**. Disponível em: https://jus.com.br/artigos/66527/insuficiencia-das-leis-em-relacao-aos-crimes-ciberneticos-no-brasil. Acesso em: 14 jun. 2022.

VIANNA, Túlio; MACHADO, Felipe. **Crimes informáticos.** Belo Horizonte: Fórum, 2013.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. Crimes Cibernéticos. [S.l.]. Rio de Janeiro: Brasport, 2013.

ZAFFARONI, Eugenio Raúl. A questão criminal / Eugenio Raúl Zaffaroni; tradução Sérgio Lamarão. – 1. ed. – Rio de Janeiro: Revan, 2013.