PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE DIREITO E RELAÇÕES INTERNACIONAIS
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO
ARTIGO CIENTÍFICO

CRIMES VIRTUAIS

A EVOLUÇÃO DOS CRIMES CIBERNÉTICOS E OS DESAFIOS NO COMBATE

ORIENTANDO (A): MATEUS ISRAEL ALVES CRUVINEL BARBOSA
ORIENTADOR (A): PROF. MA TATIANA TAKEDA

GOIÂNIA
2020

MATEUS ISRAEL ALVES CRUVINEL BARBOSA

CRIMES VIRTUAIS

A EVOLUÇÃO DOS CRIMES CIBERNÉTICOS E OS DESAFIOS NO COMBATE

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito e Relações Internacionais, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUCGOIÁS).

Prof.ª Orientadora: MA. Tatiana de Oliveira Takeda

GOIÂNIA

2020

MATEUS ISRAEL ALVES CRUVINEL BARBOSA

CRIMES VIRTUAIS

A EVOLUÇÃO DOS CRIMES CIBERNÉTICOS E OS DESAFIOS NO COMBATE

Data da Defesa: ____ de _____ de 2020.

BANCA EXAMINADORA

_____

Orientador: Prof. Titulação e Nome Completo Nota

_____

Examinador Convidado: Prof. Titulação e Nome Completo Nota

Dedico esse trabalho de conclusão de curso primeiramente a Deus, pois em nenhum momento faltou a sua guia e luz.
Dedico também a toda minha família, pelo esforço incessável em fazer tudo isso possível.

Agradeço a DEUS, por ser o meu sustento, que me deu força, sabedoria, guia e luz para vencer todos os obstáculos e dificuldades que se levantaram, e sempre foi o meu socorro bem presente.
Ao meu tio Elias, que usado por Deus, e graças ao seu incessável esforço, viabilizou a abertura dessa porta para que eu pudesse estar cursando uma universidade e estar bem perto de alcançar mais uma vitória importantíssima na minha vida, serei eternamente grato.
Aos meus avós Jordelon e Benedita (*in memoriam)* e meu tio Eliseu, que também tiveram uma grande contribuição para que eu pudesse chegar até aqui.
Aos meus amados pais Israel e Poliana, que sempre me ajudaram e me apoiaram para nunca desistir dos meus sonhos e torná-los real.
Ao meu irmão Felipe, que é o meu amigo, companheiro e sempre esteve ao meu lado durante essa jornada.
À professora e orientadora Tatiana Takeda, que teve muita paciência e acreditou na realização desse trabalho, auxiliando com dicas, sugestões e fazendo correções que foram preciosas para tornar a conclusão desse trabalho possível.

SUMÁRIO

RESUMO

O presente trabalho tem por objetivo adentrar o mundo virtual, analisando como os crimes virtuais surgiram, desenvolveram e evoluíram no decorrer dos anos, além de como pode afetar os diversos usuários da tecnologia nos dias atuais. São analisadas a forma em que os crimes virtuais se apresentam no dia a dia, como eles são classificados, os sujeitos que praticam, bem como a legislação existente no Brasil para tentar combater. Também é abordada a importância de se ter uma legislação transparente, que chegue ao conhecimento dos usuários para saberem como e a quem recorrer em caso de serem vítimas, além de profissionais capacitados para lutar contra esse mal.

Palavras-chave: Crimes virtuais. *internet. Legislação. Combate.*

ABSTRACT

This work aims to enter the virtual world, analyzing how virtual crimes arose, developed and evolved over the years, in addition to how it can affect the various users of technology today. The way in which virtual crimes are presented on a daily basis, how they are classified, the subjects they practice, as well as the existing legislation in Brazil to try to combat are analyzed. It also addresses the importance of having transparent legislation, which comes to the knowledge of users to know how and who to turn to in case of being victims, in addition to professionals trained to fight against this evil.

Key-words:. *Virtual crimes. Internet. Legislation. Combat.*

CRIMES VIRTUAIS

A EVOLUÇÃO DOS CRIMES CIBERNÉTICOS E OS DESAFIOS NO COMBATE

Mateus Israel Alves Cruvinel Barbosa

INTRODUÇÃO

É muito comum ouvir que se vive atualmente a era da tecnologia, a qual evolui cada vez mais. A base disso é a *internet*, uma ferramenta que se tornou indispensável ao dia a dia de qualquer pessoa, seja no âmbito profissional, pessoal, acadêmico e outros, mas que também é usada para a prática de crimes, conhecidos como crimes virtuais ou cibernéticos.

Sendo assim, o presente trabalho tem por objetivo mostrar como ocorrem os crimes cibernéticos, quais os meios utilizados para a prática dos crimes, quem são os sujeitos que praticam e qual a legislação vigente para combater.

A primeira seção visa mostrar como surgiu a *internet*, qual era o seu intuito e como ela evolui até se tornar essa poderosa ferramenta, pois muitas pessoas fazem uso sem ter a noção do perigo que estão expostas diariamente, seja em seu computador, smartphone ou qualquer outro meio.

Assim como existem pessoas capacitadas que ano após ano conseguem melhorar e trazer inovações tecnológicas, existem aqueles que usam desse conhecimento para tirar proveito de outras pessoas que muita das vezes são leigas no assunto, e daí surgem as vítimas dos crimes virtuais.

A segunda seção tem o objetivo de esclarecer o que são os crimes virtuais, a sua evolução, como se fazem presente atualmente e quem pode estar por trás dessa prática.

O surgimento dessas práticas ilícitas torna necessário a interferência do direito na tecnologia, para garantir que os usuários tenham segurança ao acessar um *site,* um aplicativo, uma rede social etc.

Sendo assim, é indispensável que nos tempos atuais, os usuários estejam antenados na maneira em que esses crimes ocorrem e qual a legislação vigente no país atualmente que visa oferecer essa segurança.

A terceira seção aborda qual a legislação vigente no território nacional e o seu papel no combate aos crimes virtuais.

SEÇÃO 1
O SURGIMENTO DA *INTERNET*

1.1 – BREVE HISTÓRICO

A *internet* é um fenômeno mundial, e tornou-se indispensável ao cotidiano das pessoas, seja como ferramenta para trabalhar, estudar, formas de lazer, dentre outras inúmeras funções. Segundo a organização das Nações Unidas, até o final do ano de 2018, cerca de 51,2% da população usava a internet, correspondendo assim a 3,9 bilhões de pessoas no mundo todo (Globo, 2018, *online).* Porém, onde teve início essa ferramenta que se tornou indispensável a sociedade em geral?

Obviamente a *internet* não surgiu como temos acesso a ele hoje em dia, e provavelmente nem mesmo o seu criado imaginava as proporções que tomariam, onde se costuma dizer atualmente que estamos vivendo a era da tecnologia, e a internet é justamente um desses fatores que nos possibilitou ter uma tecnologia tão avançada como temos acesso, podendo usá-la nos computadores, celulares e demais aparelhos.

Ela foi criada no ano de 1969, porém obviamente, era bem diferente do que estamos usualmente acostumados e com outros objetivos. Esse período estava ocorrendo a chamada guerra fria sendo os dois principais envolvidos o Estados Unidos e a União Soviética, então os norte americano criaram um sistema para

descentralizar suas informações no Pentágono, temendo possíveis ataques que poderiam causar perdas importantes de documentos do governo, e foi quando então o Departamento de Defesa dos Estados Unidos (ARPA – *Advanced Research Projects Agency*) e criou uma rede, que na época foi chamada de *Arpanet*, e a sua função era dividir informações em pacotes pequenos que contêm trechos dos dados, os endereços para onde seriam enviados as mensagens e informações, além de permitir também que a mensagem pudesse ser remontada, adquirindo assim a sua forma original . Nesse mesmo ano, um professo da Universidade da Califórnia passou um e-mail para um amigo em *Stanford*, o que seria o primeiro e-mail da história (Diana, 2019, *online).*

Pode-se ver então, que a ideia inicial já era o armazenamento de informações, além de também possibilitar que pessoas de diferentes espaços físicos pudessem se relacionar.

As décadas seguintes foram fundamentais para que a *internet* começasse a tomar o rumo que tem hoje, quando foram criados os protocolos TCP/IP através de trabalhos experimentais realizado em conjunto pela ARPA e demais agências (Barros, 2019, *online).*

A partir, portanto, do ano de 1973, ganhou-se essa nomenclatura com a qual estamos tão acostumados hoje em dia e a internet começou a ganhar a “cara” que podemos encontrar atualmente.

Em 1982, a *Internet* adentrou também o âmbito acadêmico e permaneceu por aproximadamente 20 anos sendo restrita ao meio acadêmico e científico. Inicialmente de uso restrito dos Estados Unidos, chegou posteriormente na Europa, em países como Holanda, Dinamarca e Suécia. Apenas em 1987 foi usada pela primeira vez para uso comercial nos Estados Unidos (Silva, 2001, *online*).

Para quem estudou nos tempos antigos, estavam talvez acostumados a realizar pesquisar em livros, passar horas e horas em bibliotecas, mas o que seria do estudante moderno sem o acesso à *internet*, já que nos possibilita realizar pesquisas acadêmicas, encontrar livros e demais facilidades que estamos habitualmente acostumados, além também de ter adentrado no âmbito comercial, onde encontramos a facilidade de comprar e vender sem sair do conforto de nossas casas.

Foi na década de 1990 que a *internet* começou a ter os primeiros esboços do que se tornaria nos dias de hoje, quando o cientista, professor e físico britânico

Tim Berners-Lee desenvolveu um navegador ou *browser* como também é conhecido, a *World Wide Web*, o popular “www” que precede os sites, rede mundial de Computadores. A partir de então ela se popularizou pelo mundo com surgimento de novos browsers, muito conhecidos atualmente, como a *internet Explorer*, *Mozilla Firefox*, *Google Chrome*, *Opera*, dentre outros e consequentemente o aumento de usuários. Diante de tudo isso, começa a proliferar *sites*, *chats* e as famosas redes socias (Diana, 2019, *online).*

Começava ali um esboço do que se tornaria a *internet*, uma potente ferramenta com navegadores e redes sociais que se tornaram indispensáveis nas rotina atualmente.

Com a chegada das famosas redes sociais, a internet alcançou um novo patamar de usabilidade e interação entre pessoas do mundo todo. A primeira surgiu em 1995 chamada de *classmates*, uma página que possibilitava troca de conhecimentos e marcar encontros entre estudante do Estados Unidos e Canadá, rede social esta que chegou a ter 50 milhões de usuários. Em 2002 foi a vez do fotolog, a qual conta com mais de 32 milhões de usuários espalhados em 200 países, tendo como objetivo o compartilhamento de fotos (Diana, 2019, *online*).

Surge então as aclamadas redes sociais, sendo quase impossível imaginar um mundo nos tempos atuais sem *instagram*, *facebook*, *whatsapp*, entre outros, aplicativos esses que vieram para revolucionar o mundo e mudar as nossas vidas, possibilitando uma interação entre pessoas no mundo todo e uma maneira ágil de espalhar notícias e acontecimentos, mobilizar pessoas em prol de causas nobres e campanhas, fazendo com que todos tenham acesso aos acontecimentos do mundo todo, porém, tudo isso tornou-nos “escravos” das redes e fez uma sociedade dependente da informática, sendo assim, é cada vez mais difícil ter controle sobre o mundo virtual.

1.2 A INTERNET NO BRASIL

Geralmente, as tecnologias são criadas primeiro em países conhecidos como desenvolvidos e posteriormente vão se espalhando para o restante do mundo. Sendo assim, no Brasil a internet chegou na década de 80.

Foi então através de iniciativa da FAPESP (Fundação de Amparo à Pesquisa do Estado de São Paulo), UFRJ (Universidade Federal do Rio de Janeiro) e LNCC (Laboratório Nacional se Computação Científica) quando as universidades brasileiras passaram a manter compartilhamento de informações com os Estados Unidos. A LNCC conseguiu acesso a *bitnet* em setembro de 1988, por meio de uma conexão com o FERMILAB (*Fermi National Accelerator Laboratory*) em Chicago. Depois, a FAPESP criou a rede ANSP (*Academic Network at São Paulo*), que interligava a Universidade de São Paulo, a Universidade de Campinas, a Universidade Estadual Paulista e o Instituto de Pesquisas Tecnológicas do Estado de São Paulo. Algum tempo depois, essa ligação chegou até a Universidade Federal de Minas Gerais e a Universidade Federal do Rio Grande do Sul, e assim foi crescendo essa ligação com demais universidades (Muller, 2019, *online*).

No Brasil, a *internet* chegou, portanto, primeiro no âmbito acadêmico, mais precisamente nas universidades em São Paulo, onde usaram dessa rede para se relacionar com demais universidades em outros lugares do mundo. Como por exemplo nos Estados Unidos e posteriormente essa ligação foi crescendo e expandindo também para as demais universidades do país.

Em 1981, foi fundado o IBASE (Instituto Brasileiro de Análises Sociais e Econômicas), tendo como um dos seus objetivos a disseminação de informações a sociedade civil. Isso incluía a democratização do acesso às redes de computadores no país. Em meados da década de 80, o IBASE integrou a um projeto internacional chamado *interdoc*. Sua função era o uso do correio eletrônico para o intercâmbio de informações entre ONG´s, de todo o mundo. Porém, esse projeto era muito caro, fazendo-se necessário buscar por meios alternativos para possibilitar essa conexão internacional reduzindo os custos (Muller, 2018, *online*).

Até então, a *internet* era usado somente no meio acadêmico, mas logo buscou-se maneiras de expandir esse uso para demais atividades, chegando

portanto o *alternex*, um serviço internacional de mensagens e conferências eletrônicas pioneiras no país

Por meio do *alternex*, passou a ser possível a troca de mensagens com diversos sistemas de correio eletrônico de todo o mundo, incluindo a *internet*. Assim, o *alternex* foi o primeiro serviço brasileiro de acesso à *internet* fora do âmbito acadêmico (Muller, 2018, *online*).

E com o grande sucesso que teve, o governo então via na *internet* uma forma de desenvolvimento do país, que somente traria benefícios.

Quase no final do ano de 1994, o governo brasileiro passou a divulgar a intenção de investir na nova tecnologia, através do Ministério de Ciência e Tecnologia e do Ministério das Comunicações. A Embratel e a RNP ficaram responsáveis pela criação da estrutura necessária para exploração comercial da *internet*. A Embratel então iniciou seu serviço de acesso a *internet* de forma experimental, escolhendo 5 mil usuários para testar o serviço. Em maio de 1995, o acesso à *internet* através da Embratel começou funcionar de modo definitivo. Para evitar o monopólio no mercado, o governo brasileiro anunciou então que o mercado de serviços da internet seria o mais aberto possível (Muller, 2018, *online)*

Porém, o que até então ainda era um serviço muito limitado, começaria o seu age a partir do ano de 1996, quando recebeu melhorias para começar a caminhar para o que é hoje, com a crescente no número de usuários.

O acesso em todo território nacional expandiu-se através das redes locais de conexão, no ano de 1997 e, dessa forma, a internet então foi cada vez mais crescendo e evoluindo até se tornar o que hoje conhecemos (Diana, 2019, *online*).

Segundo dados divulgados pelo Ministério da Ciência e Tecnologia em 2011, constatou-se que aproximadamente 80% da população teve acesso à *internet*, correspondendo, portanto, a 60 milhões de computadores em uso.

Apesar de a *internet* ter tomado grandes proporções apenas na década de 90, o Brasil, porém passou a ser um dos países que mais utiliza essa ferramenta, sendo o quarto país com mais usuários, atrás apenas de países como China, índia e Estados Unidos, países estes que possuem uma população maior em comparação com o nosso. Mas, através disso, podemos perceber o quanto a população tem se tornado dependente, e já não sabem, ou até mesmo não podem viver sem ela.

Porém, assim como é uma ferramenta que nos ajuda e auxilia, o seu uso descontrolado tem tornado cada vez mais difícil o controle ao acesso e a maneira

como muitos utilizam, e assim como tem aqueles que usam suas habilidades e conhecimentos para o bem, há também os que usam para tirar proveito das situações, surgindo portanto os crimes no âmbito virtual também, o qual será abordado à seguir.

SEÇÃO 2
CRIMES VIRTUAIS E DESAFIOS NO COMBATE

2.1 A EVOLUÇÃO DOS CRIMES CIBERNÉTICOS

Crimes virtuais ou cibernéticos como também são conhecidos, são crimes no qual a ferramenta utilizada para praticá-los é a *internet*, conforme BRASIL (p. 23, 2008):

> Crime virtual ou crime digital pode ser definido como sendo termos utilizados para se referir a toda a atividade onde um computador ou uma rede de computadores são utilizados como uma ferramenta, uma base de ataque ou como meio de crime. Infelizmente, esta prática tem crescido muito já que esses criminosos virtuais têm a errada impressão que o anonimato é possível na Web e que a Internet é um “mundo sem lei.

Atualmente é muito comum deparar-se com esses tipos de crimes, como por exemplo furto de dados, invasão de dispositivo informático, dentre outros que serão vistos posteriormente, e assim como a internet tomou uma grande proporção, as práticas de crimes cibernéticos são cada vez mais frequentes, pois esses criminosos encontram na *internet*, uma maneira de se esconder “atrás” de um computador ou até mesmo acreditam que a punição para esse tipo de crimes acaba sendo menos severa do que deveria. Essa relação entre crimes e internet começou na década de 1960, concomitantemente a criação da *internet*, de acordo com GUIMARÃES (2003, p 68):

> Segundo Ferreira, o surgimento dos crimes informáticos remonta, no entender de Ulrich Sieber, da Universidade de Wurzburg, à década de 1960,

> época em que apareceram na imprensa e na literatura científica os primeiros casos de uso do computador para a prática de delitos, constituídos, sobretudo, por manipulações, sabotagens, espionagem e uso abusivo do de computadores e sistemas, denunciados em matéria jornalística. Somente na década seguinte é que se iniciaram os estudos sistemáticos e científicos sobre essa matéria, com emprego de métodos criminológicos, analisando-se um limitado número de delitos informáticos que haviam sido denunciados, entre os quais alguns casos de grande repercussão na Europa por envolverem empresas de renome mundial.

Certamente quando surgiu a internet, e assim como ela foi se desenvolvendo e caminhando para a poderosa ferramenta que se tornou, auxiliando em afazeres nas rotinas de trabalho, lazer e demais opções, não previram que poderia se tornar também uma “arma” poderosa para a prática criminal e, infelizmente, todo esse conhecimento brilhante de uma mente humana se desenvolveu não apenas para o bem, mas também para caminhos delituosos. Sendo assim, com o passar dos anos, as ações criminosas começaram a se manifestar e tomar a forma que se apresentam nos dias de hoje, conforme GUIMARÃES (2003, p 68):

> A partir de 1980, ressalta a autora o aumento de ações criminosas que passaram a incidir em manipulações de caixas bancárias, pirataria de programas de computador, abusos nas telecomunicações etc., revelando a vulnerabilidade que os criadores de processo não haviam previsto. Acrescente-se, ainda, o delito de pornografia infantil na rede, igualmente difundido na época.

A relação de crimes que podem ser praticados através da *internet* é extensa, mas existem aqueles que acontecem com maior frequência, como o *phishing, spam* e *malwares.*

2.2 TIPOS DE CRIMES CIBERNÉTICOS

Os crimes cibernéticos podem ser divididos em tipos. Oss meio mais comuns para se praticar um crime virtual é através do *phishing*, *spam* ou *malware.*

P*hishing* são conversas ou mensagens falsas com *links* fraudulentos *que* ocorre através de e-mail de *spam* ou outras formas de comunicação que são

enviadas no atacado com o intento de induzir aqueles que recebem, a fazer algo que prejudique a segurança pessoal ou da organização onde trabalham. As mensagens falsas enviadas muitas das vezes contêm anexos infectados ou links que redireciona a vítima para *sites* maliciosos. Existe ainda o *spear-phishing,* que é quando a mensagem enviada vem com o intuito de se passar por uma pessoa influente, como por exemplo o CEO da empresa.

Spam, sigla utilizada para *Sending and Posting Advertisement in Mass, traduzindo para o português significa "*Enviar e Postar Publicidade em Massa" se trata de mensagens enviadas sem o consentimento do usuário, ou seja, a mensagem chega sem a permissão ou desejo da vítima de receber (Alencar, 2016, *online).*

Na grande parte dos crimes, a mensagem de *Spam* promove um produto ou serviço com o intuito de que a pessoa se interesse e acaba acessando o *link* fraudulento. Mas em outros casos, o objetivo é apenas propagar uma história falsa, e ao clicar, as informações de dados financeiros e pessoais são roubadas.

Os *malwares* são *softwares* maliciosos instalados sem permissão do usuário. Vírus, cavalos de Tróia, *spywares* e *ransomwares* estão entre os diferentes tipos de *malwares* (Sumrell, *online).*

Normalmente um *malware* é desenvolvido por equipes de *trackers* que, em grande parte das vezes, tem como objetivo uma forma de ganhar dinheiro, através da proliferação do próprio *malware* ou leilão na *deep web.*

A invasão de dispositivos informáticos está prevista no artigo 154-A do Código Penal, quando um dispositivo de processamento, dispositivos de entrada ou saída são indevidamente violados.

A lei 9.610 de 1998 aborda sobre a pirataria de *software,* que é quando dados são copiados em Cd's, DVD's e outras bases de dados, sem a autorização do autor.

Além desses tipos de crimes, o meio virtual pode ser usado ainda para a prática de outras ações criminosas, como a divulgação de informações falsas e mentirosas, devido a *internet* ter se tornado um meio de rápida proliferação de notícias, podendo até mesmo ser classificado como difamação, calúnia e injúria.

Difamação é imputar a alguém fato, com circunstâncias descritivas, ofensiva a sua reputação, por meio da *internet.*

A calúnia, como por exemplo as *fake News*, popularmente conhecida atualmente, é a divulgação de notícias falsa.

E injúria ou também conhecido no meio virtual como *cyberbulliying,* é ofender a dignidade de alguém através da *internet.*

Estes crimes estão previstos nos artigos 138, 139 e 140 respectivamente do Código Penal.

Outra prática muito comum nos dias de hoje, é a divulgação de conteúdo sexual, sem a permissão da pessoa envolvida, podendo ocorrer até mesmo casos de pedofilia.

Muitos sites criam conteúdos que abordam explicitamente atos sexuais cujos participantes são menores de idade, além de fotos de nudez e cenas para satisfação de desejos sexuais dos criminosos.

Esses crimes estão previstos nos artigos 241-A e 241-E da lei 8.069/90 onde caracterizam como crime as ações de oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por meio de sistema de informática, fotografia, vídeo ou outro registro que contenha qualquer situação que envolva criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou exibição dos órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais.

O artigo 213 do Código Penal, prevê também como crime constranger alguém, com uma chantagem por *hacking* de computação ou ameaça qualquer, até mesmo por uma webcam, com refém, por exemplo, a satisfazer a lascívia por videoconferência, por meio de prática de um ato libidinoso diverso de conjunção carnal (Schaun, 2018, *online*).

É considerado ainda como crime virtual a incitação ou apologia ao crime utilizando-se da internet, conforme previsto nos artigos 286 e 287 do Código Penal.

2.3 – CLASSIFICAÇÃO DOS SUJEITOS QUE PRATICAM

Os sujeitos que praticam esses tipos de crimes podem ser tanto pessoas com conhecimento mais aprofundando, como os *crackers* ou também pessoas

“normais”, que são qualquer pessoa que cometem crimes umas contra as outras, através de suas condutas na *internet.*

Mesmo *o*s *hackers* sendo sempre associados a sujeitos que praticam crimes através da *internet,* esse é um conceito equivocado, pois *hackers* são qualquer pessoa que se dedique em alguma área específica da computação para descobrir utilidades além das que já são previstas nas especificações originais (Ultradownloads, *online).*

Os verdadeiros criminosos são os conhecidos como *crackers,* que usam seus conhecimentos para violar sistemas ou redes de computadores.

Porém, como foi visto nos tipos de crimes, há crimes virtuais que qualquer pessoa pode cometer, como por exemplo, incitação ou apologia ao crime, *cyberbullying*, entre outros.

SEÇÃO 3
O PAPEL DA LEGISLAÇÃO VIGENTE

O Brasil sempre foi muito criticado por não haver uma legislação específica à respeito de crimes virtuais ou cibernéticos, ou mesmo com a legislação existente, ainda ser um país que sofre constantemente com a prática de crimes virtuais, e os infratores acabam saindo ilesos, pois muitas das pessoas são leigas e não sabem nem mesmo como proceder em caso de serem vítimas.

As leis que regem o Brasil são o Marco civil da *internet,* a Lei Carolina Dieckmann e o Lei Geral de Proteção de Dados (LGPD) que acaba de entrar em vigor.

3.1 – MARCO CIVIL DA *INTERNET*

O marco civil da *internet* é a Lei n^{o} 12.965/2014 que entrou em vigor no desde o dia 23 de junho de 2014 e regulamenta o uso da *internet.*

Ela é responsável por estabelecer princípios e garantias para que a rede possa ser livre e democrática no Brasil. Ela que dita os direitos e deveres dos usuários e empresas provedoras de acesso e serviços *online* (Martins, 2015, *online).*

Assim como em qualquer meio que alguém esteja inserido há princípios a serem seguidos, no mundo virtual não é diferente, e para que haja uma harmonia entre os provedores e usuários e evite que alguém seja prejudicado, essa lei também tem o papel de reger os deveres de que provê esse tipo de serviço.

O marco civil da *internet* proíbe que os provedores de telecomunicações restrinjam conexão e velocidade de acordo com o conteúdo, origem, destino e serviço acessado pelo usuário, ou seja, garantindo assim a mesma qualidade de acesso à rede para todos (Martins, 2015, *online).*

3.2 – LEI CAROLINA DIECKMANN

A Lei n^{o} 12.737/2012 ou Lei Carolina Dieckmann, é voltada a punição de crimes virtuais. Ela ganhou esse nome devido ao fato de que na época em que o projeto tramitava na Câmara de Deputados, a atriz brasileira acabou sendo vítima de um crime cibernético, tendo fotos pessoais divulgadas sem a sua autorização (Uol, 2013, *online).*

Essa lei veio para alterar o código penal, tipificando como infração várias condutas no meio virtual, tendo como principal foco, a invasão de computadores, que se tornou algo recorrente, e visa também estabelecer punições específicas, algo que não existia até a criação dessa lei.

Casos como esse da atriz, que antes muita das vezes ficavam impune, passou a ser o foco da Lei Carolina Dieckmman.

Portanto, para que seja enquadrado nessa lei, é necessário que haja invasão em computadores, tablets, celulares e demais aparelhos eletrônicos, mesmo estando ou não conectado à *internet,* com o intuito de obter, adulterar ou destruir dados ou informações.

A lei tipifica como crime invadir dispositivo alheio, conectado ou não a rede de computadores, mediante violação de segurança com o fim de obter

informações sem autorização, e tem como pena a detenção de três meses a um ano e multa. Tem ainda como agravante roubo de informação em que causa prejuízo econômico, aumentando a pena de detenção de três meses a um ano e quatro meses, obtenção de conteúdo de comunicações privadas de formas não autorizada, tendo como pena de seis meses a dois anos e multa e por último divulgação e comercialização de conteúdo roubado de dispositivo informático, tendo como pena a reclusão de oito meses a três anos e quatro meses (Uol, 2013, *Online).*

Mesmo que tenha trago punições específicas, essa lei foi alvo de críticas em relação as penas, pois são consideradas muito brandas. Além disso, outro problema que apontam especialistas do direito digital, é que para que haja a consumação do crime, o infrator deve passar por alguma barreira de segurança, ou seja, se alguém usa um computador que não esteja travado com senha para roubar dados, ele não pude ser punido.

Mesmo que ainda haja algumas questões a serem resolvidas, como essas que foram alvo de críticas, a respeito das penas, é inegável que essa lei significou um grande avanço no combate aos crimes virtuais.

3.3 – LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

A Lei Geral de Proteção de Dados (LGPD) foi aprovada em 2018 pelo então presidente Michel Temer e estava prevista para entrar em vigor dois anos depois, porém, a medida provisória 959/20 tentou adiar esse prazo, mas acabou sendo derrubada pelo Senado Federal. Dessa forma, a LGPD entrou em vigor, logo que a lei de conversão da Medida Provisória foi promulgada, situação esta que ocorreu no dia 19 de setembro de 2020.

Essa nova lei visa criar um cenário de segurança jurídica, tornando uniforme as normas e práticas, para que possa ser promovida a proteção de forma igual dentro e fora do país, aos dados pessoais de todos os cidadãos que estejam no Brasil. Ela define como dados pessoais todas as informações que possam identificar de forma direta ou indireta um indivíduo vivo, como por exemplo Rg, CPF, gênero, data e local de nascimento, telefone, endereço residencial, localização via

GPS, retrato em fotografia, prontuário de saúde, cartão de banco, renda, histórico de pagamentos, hábitos de consumo, preferencias de lazer, endereço de Protocolo da *Internet* e *cookies,* entre outros (Serpro, 2020, *online).*

As crianças e adolescentes merecem um cuidado especial, e por isso ficou definido que esses dados exigem um cuidado ainda mais cauteloso, conhecidos como dados sensíveis e que sejam eles tratados no meio físico ou digital, estando sujeitos a regulamentação.

A LGPD deve ser cumprida independente de a sede da organização ou o centro de dados ser no Brasil ou não, quando o processamento de dados for sobre pessoas que estiverem em solo brasileiro, mesmo que não seja brasileiro e em caso de compartilhamento de dados com organizações internacionais ou outros países, é necessário que tenha protocolos para garantir a segurança e o cumprimento de exigências legais (Serpro, 2020, *online).*

A nova lei trouxe um ponto importante, que é o consentimento, ou seja, para que dados pessoais possam ser tratados, é fundamental que tenha o consentimento do cidadão.

Porém, há exceção para os casos em que for indispensável para cumprir uma obrigação legal, executar políticas públicas prevista em lei, realizar estudos através de órgãos de pesquisa, executar contratos, defender direitos em processo, preservar a vida e a integridade física de uma pessoa, tutelar ações feitas por profissionais das áreas da saúde pública ou sanitária, prevenir fraudes contra o titular, proteger o crédito ou atender a um interesse legítimo, contanto que venha a ferir os direitos fundamentais do cidadão (Serpro, 2020, *online).*

Essa proteção se estende também aos diretos do cidadão, que pode requerer que dados sejam apagados, pode desistir do consentimento, transferir dados para outro fornecedor de serviços, entre outros, além de que o tratamento de dados tem que ser feito respeitando alguns quesitos, como a finalidade e a necessidade, que devem ser acertados e informados ao cidadão antes de ter acesso aos dados.

Ficou estabelecido que o órgão responsável pela fiscalização será a Autoridade Nacional de Proteção de Dados Pessoais (ANPD).

Essa instituição ficará responsável pela fiscalização e, em caso de descumprimento da lei, poderá penalizar. Fica a cargo da ANPD também regular e orientar como a lei deve ser aplicada.

E por último, a LGPD tem também o papel de administrar os riscos e falhas, ou seja, os responsáveis por administrar a base de dados pessoais deve elaborar normas de administração, cumprir medidas de segurança e em caso do vazamento dos dados, a ANPD e as pessoas envolvidas devem ser avisados imediatamente.

As falhas de segurança podem gerar multas de até 2% do faturamento anual da organização no Brasil, e no limite de 50 milhões por infração. Os níveis de penalidades serão fixados pela autoridade nacional de acordo com o grau da falha. E enviará alertas e orientações antes de aplicar sanções as organizações (Serpro, 2020, *online).*

CONSIDERAÇÕES FINAIS

Ao fim da pesquisa, pode-se concluir a importância de saber como os crimes virtuais estão presente no dia a dia, por mais que muita das vezes, o pensamento é de que só acontece com o próximo, mas ninguém está imune, pois como foi visto, vítimas são feitas simplesmente ao acessar um *link*.

Na primeira seção, nota-se que apesar do objetivo de criação da *internet* ser algo totalmente diferente do que se tem acesso atualmente, essa ferramenta evoluiu e tomou proporções em que é inimaginável um mundo sem a tecnologia.

A segunda seção deixa o leitor antenado em como os crimes virtuais podem ser praticados, além de mostrar também quem são os responsáveis por causar esse dano.

A terceira seção ajuda a entender como as leis trabalham para combater os crimes virtuais e quais são os desafios enfrentados, pois, apesar de agora ter uma legislação específica, ainda restam muitas lacunas a serem preenchidas. Todavia, pode-se ver o grande avanço no combate aos crimes cibernético, com legislações mais claras e que visam garantir a segurança dos usuários e punir os *cyber* criminosos.

O trabalho alcançou o seu objetivo de expor a prática dos crimes virtuais e a maneira como ocorrem, para que os usuários possam saber como se prevenir, e

se caso forem feitas vítimas, saibam como recorrer ao judiciário e buscar respaldo na legislação, pois assim como a tecnologia avança, buscam-se também novas formas de trazer mais segurança aos usuários, criando leis e fiscalizando o uso.

REFERÊNCIAS

ANDREI, Lucas. **A história da internet – Do Início ao Status Atual da Rede**. Web Link, 2019. Disponível em: https://www.todamateria.com.br/referencia-site-abnt/. Acesso em: 03/06/2020

BARRETO, Alesandro Gonçalves. BRASIL, Beatriz Silveira. **Manual de Investigação Cibernética à Luz do Marco Civil da Internet.** Editora Brasport. Rio de Janeiro. 2016.

BARROS, Thiago. **Internet completa 44 anos; relembre a história da web**. Techtudo, 07 abr. 2013. Disponível em: https://www.techtudo.com.br/artigos/noticia/2013/04/internet-completa-44-anos-relembre-historia-da-web.html. Acesso em: 03/06/2020

DIANA, Daniela. **História da Internet.** Toda Matéria. Disponível em: https://www.todamateria.com.br/historia-da-internet/. Acesso em: 12/06/2020

GLOBO. **Mais da metade da população mundial usa internet, aponta ONU**. Globo, 07 dez. 2018. Economia. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2018/12/07/mais-da-metade-da-populacao-mundial-usa-internet-aponta-onu.ghtml. Acesso em: 01/06/2020.

GOV.BR. **Serpro e LGPD: segurança e inovação**. Gov.br. Disponível em: https://www.serpro.gov.br/lgpd. Acesso em: 23/09/2020

MARTINS, Geiza. **O que é o marco civil da internet?.** Super interessante, 4 jul. 2018. Disponível em: https://super.abril.com.br/mundo-estranho/o-que-e-o-marco-civil-da-internet/. Acesso em: 23/09/2020

NETO, Mário; GUIMARÃES, José. **Crimes na Internet: elementos para uma reflexão sobre ética informacional.** Brasília. 2003.

SCHAUN, Guilherme. **Uma lista com 24 crimes virtuais**. Jusbrasil, 2018. Disponível em: https://guilhermebsschaun.jusbrasil.com.br/artigos/686948017/uma-lista-com-24-crimes-virtuais. Acesso em: 21/09/2020

SILVA, Leonardo. **Internet foi criada em 1969 com o nome de "Arpanet" nos EUA.** Folha de S. Paulo, São Paulo, 12 ago. 2001. Disponível em: https://www1.folha.uol.com.br/folha/cotidiano/ult95u34809.shtml. Acesso em: 03/06/2020.

SUMRELL, Mariano. **O que é vírus, cavalo de tróia, spyware, etc?.** Canaltech. Disponível em: https://canaltech.com.br/seguranca/O-que-e-virus-cavalo-de-troia-spyware-etc/. Acesso em: 20/09/2020

ULTRADOWNLOADS. **O que é um hacker?.** Canal Tech. Disponível em https://canaltech.com.br/hacker/O-que-e-um-Hacker/. Acesso em: 22/09/2020

UOL. **Lei Carolina Dieckmann sobre crimes na internet entra em vigor**. Uol, 02 abr. 2013. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2013/04/02/lei-carolina-dieckmann-sobre-crimes-na-internet-entra-em-vigor.htm. Acesso em: 23/09/2020