UNIVERSIDADE FEDERAL DO RIO DE JANEIRO

CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS

FACULDADE DE DIREITO

OS CRIMES CIBERNÉTICOS E A INEFICÁCIA DA LEI CAROLINA DIECKMANN NO AMBITO DO DIREITO PENAL

GABRIELLA SOUZA DE ALCANTARA

Rio de Janeiro

2022.2

GABRIELLA SOUZA DE ALCANTARA

OS CRIMES CIBERNÉTICOS E A INEFICÁCIA DA LEI CAROLINA DIECKMANN NO AMBITO DO DIREITO PENAL

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de Bacharel em Direito, sob a orientação da **Professora Dra. Cristiane Brandão Augusto Mérida.**

Rio de Janeiro

2022.2

CIP - Catalogação na Publicação

A347c

Alcantara , Gabriella Souza de
Crimes cibernéticos e a ineficácia da lei Carolina dieckmann no âmbito do direito penal / Gabriella Souza de Alcantara . -- Rio de Janeiro, 2022.
50 f.

Orientadora: Cristiane Brandão Augusto Mérida .
Trabalho de conclusão de curso (graduação) - Universidade Federal do Rio de Janeiro, Faculdade Nacional de Direito, Bacharel em Direito, 2022.

1. Crimes Cibernéticos . 2. Direito Penal . 3. Carolina Dieckmann. I. Mérida , Cristiane Brandão Augusto , orient. II. Titulo.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a), sob a responsabilidade de Miguel Romeu Amorim Neto - CRB-7/6283.

GABRIELLA SOUZA DE ALCANTARA

OS CRIMES CIBERNÉTICOS E A INEFICÁCIA DA LEI CAROLINA DIECKMANN NO AMBITO DO DIREITO PENAL

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de Bacharel em Direito, sob a orientação da **Professora Dra. Cristiane Brandão Augusto Mérida.**

Data da Aprovação: __ / __ / ____.

Banca Examinadora:

_____

Orientador

_____

Co-orientador (Opcional)

_____

Membro da Banca

_____

Membro da Banca

Rio de Janeiro

2022.2

"Desconfie daquilo que você lê na internet"

Aristóteles

AGRADECIMENTOS

Primeiramente gostaria de agradecer a Deus, pois ele sempre esteve e está comigo e essa graduação é um verdadeiro presente que ele me deu, nas noites de estudo e ansiedade, quando os pensamentos de “será que vou conseguir?” surgiam, ele sempre me acalmava e bradava ao meu coração que tudo é possível ao que crê.

Sou muito grata aos meus pais, Hilda Silva e João Batista, por todo apoio durante a minha trajetória, por todo amor e dedicação que me oferecem e por sonharem juntamente comigo e acreditarem que eu alcançaria os meus objetivos.

Agradeço ao meu irmão Jorge Alcantara por todo carinho e cuidado que sempre teve comigo, a minha cunhada Aline Ribeiro por aguentar meus desabafos durante toda a minha trajetória. Aos meus sobrinhos Júlio, Rafael e Vitor minha gratidão por todo amor e cumplicidade que temos.

Ao meu irmão de coração Bruno Neves, pela amizade e cuidados de sempre e principalmente por estudar junto comigo sempre que preciso, eu sei que com ele eu posso contar sempre.

Aos meus amigos queridos que tive o prazer de conhecer na FND e compartilhamos momentos marcantes, em especial minha gratidão a Thais, a melhor amiga que alguém poderia ter nesse mundo.

Agradeço também aos meus amigos que antes mesmo da concretização de um sonho, sonharam juntamente comigo, Isabella, Cássia, Isabelle e Monique.

Minha gratidão a Hesthefani por sua amizade e carinho.

Agradeço à minha orientadora, Cristiane Brandão Augusto Mérida, por toda dedicação, paciência e explicações que me disponibiliza, a senhora é um exemplo dentro e fora de sala de aula. A você, serei eternamente grata. Por todos os ensinamentos. Por fim, porém não menos importante, agradeço à Faculdade Nacional de Direito e à todos seus funcionários, que me

proporcionaram cinco anos inesquecíveis e essenciais em minha vida, que mudaram meu jeito de ser e de encarar a vida e me transformaram em uma mulher com pensamentos mais altruístas, além de me fazer todos os dias, ter vontade de exercer o Direito e a Justiça

RESUMO

O presente trabalho traz uma nova análise sobre a história da internet e o surgimento dos crimes cibernéticos, à luz dos atuais conceitos dessa nova medida de criminalidade, consequência das crescentes inovações tecnológicas. Além de buscar analisar a tipicidade das condutas mais comuns e mais danosas aos bens jurídicos que o Direito dispõe-se a proteger, principalmente ao ciberespaço, serão analisadas as vendas de fotos na internet, crimes contra a honra, a fake news, furto qualificado e o estelionato, que é um tipo peculiar de fraude. A invasão de privacidade, sob a ótica da Lei 12,737/2012, mais conhecida como Lei Carolina Dieckmann, que foi criada com o objetivo de proteger as informações pessoais e os dados dos usuários digitais de invasores com más intenções. No mais, tem também como objetivo vislumbrar a evolução do Direito brasileiro no tratamento dessas condutas delitivas, analisar o crescente aumento dos crimes e o tratamento que o Judiciário realiza nessas situações tanto em relação à sua competência quanto na análise de provas. Nessa medida, buscará desenvolver as dificuldades que as autoridades policiais encontram na obtenção de provas, por se tratar de um ambiente bem desfavorável para o rastreamento das mesmas. Além disso, versará também sobre a necessidade de perícias especializadas e o instituto da produção antecipada de provas.

Palavras-chave: Crimes cibernéticos – Internet – Ambiente virtual – Ineficácia – Provas – Investigação – Competência.

ABSTRACT

This work presents a new analysis of the history of the internet and the emergence of cybercrime, in the light of current concepts of this new measure of criminality, a consequence of growing technological innovations. In addition to seeking to analyze the typicality of the most common and most harmful conducts to the legal interests that the Law is willing to protect, especially to cyberspace, sales of photos on the internet, crimes against honor, fake news, aggravated theft and embezzlement, which is a peculiar type of fraud. The invasion of privacy, from the perspective of Law 12,737/2012, better known as the Carolina Dieckmann Law, which was created with the aim of protecting the personal information and data of digital users from invaders with bad intentions. In addition, it also aims to glimpse the evolution of Brazilian law in the treatment of these criminal conducts, to analyze the growing increase in crimes and the treatment that the Judiciary performs in these situations both in relation to its competence and in the analysis of evidence. To that extent, it will seek to address the difficulties that police authorities encounter in obtaining evidence, as it is a very unfavorable environment for tracking them. In addition, it will also deal with the need for specialized expertise and the institute for the early production of evidence.

Keywords: Cyber crimes – Internet – Virtual environment – Ineffectiveness – Evidence – Investigation – Competence.

SUMÁRIO

INTRODUÇÃO

O surgimento da internet aconteceu na Guerra Fria, ao qual o departamento de defesa americano pretendia instaurar pontos estratégicos de defesa e necessitava de internet para que houvesse conexão com a rede de comunicação. Com o avanço tecnológico, a internet passou a ocupar novos espaços, como lazer, estudo, trabalho, entre outros meios de comunicação. Ademais, não somente para meios benéficos que a internet passou a ser utilizada, mas também para a prática de crimes virtuais.

O objeto desta pesquisa trata-se da análise no que concerne às problemáticas e ineficácia da Lei 12.737/12. É relevante destacar que essa lei foi um marco para que crimes ocorridos nos meios virtuais se tornassem um fato criminoso, além de ter sido um fator inicial para a discussão de penalidade em crimes virtuais. Diante disso, fica indispensável a análise sobre as vulnerabilidades da referida lei, bem como classificar os crimes cibernéticos que estão vigentes no ordenamento jurídico.

A metodologia utilizada para essa pesquisa foi a bibliográfica, ao qual foram utilizados notáveis teóricos sobre o assunto, como Tarcísio Teixeira, Fernando da Costa Tourinho Filho e Patrícia Peck Pinheiro. Com o objetivo de apresentar de forma objetiva todas as problemáticas sobre o assunto, a presente pesquisa foi dividida em três capítulos.

O primeiro capítulo foi destinado para abordar de forma histórica como foi o surgimento da internet, bem como esclarecer a chegada da internet no Brasil, informação e responsabilidade dos meios de comunicação, acessibilidade, praticidade do uso, os malefícios da internet, discorrer sobre a definição de hacker e a diferença entre hacker e cracker.

O segundo capítulo foi destinado a tipificação dos crimes cibernéticos, bem como discorrer sobre ataques de malware, ransomware, bullying virtual, fake news, como são muitos os crimes nesse âmbito, o presente trabalho buscou destacar os principais, entretanto citarei em uma pequena parte os demais crimes. Assim, discorrer sobre os impactos dos crimes cibernéticos. Nessa linha, foram utilizados os teóricos Rossini e Pinheiro.

O terceiro capítulo foi destinado a uma junção dos dois capítulos anteriores, ao qual foi abordado de forma específica sobre a ineficácia da aplicação da Lei 12.737/12, nessa linha de pesquisa foram utilizados os teóricos, o levantamento bibliográfico será composto por Fernando da Costa Tourinho Filho e Patrícia Pinheiro.

Portanto, é indispensável o destaque dos antecedentes históricos da internet e a forma como se deu a sua evolução e como algo “tão bom” a princípio pode-se tornar um ambiente utilizado para a produção de condutas delitivas. Sem dúvidas o direito está ligado em toda à evolução da sociedade. À medida em que as coisas vão se desenvolvendo, o direito vai se adaptando para trazer formas para a manutenção da justiça no âmbito virtual.

1. O BREVE HISTÓRICO DA INTERNET

É incontestável que a internet é um dos maiores fenômenos mundiais, e seu uso é de extrema importância para as pessoas, sendo utilizada para estudar, trabalhar, como entretenimento e outras formas e funções diferenciadas.

A origem da internet data de 1969, portanto ainda durante a Guerra Fria, e surgiu totalmente diferente da internet que conhecemos hoje em dia. Foi criada com objetivos militares, sendo um dos instrumentos das forças armadas norte-americanas para manter as comunicações em caso de ataques inimigos que destruíssem os meios convencionais de telecomunicações e para prevenir que possíveis ataques causassem perdas importantes de documentos do governo.

A partir disso, o Departamento de Defesa dos Estados Unidos (ARPA – Advanced Research Projects Agency) criou uma rede, que naquela época foi chamada de Arpanet, e a sua função era buscar desenvolver um sistema para descentralizar suas informações do Pentágono, dividindo informações em pacotes pequenos que continham os trechos dos dados, os endereços para onde seriam enviados, às mensagens e informações, além de permitir que as mensagens pudessem ser reeditadas, adquirindo assim a sua forma original. Ainda em 1969, um professor da Universidade da Califórnia enviou um correio eletrônico para um amigo em Stanford, o que seria o primeiro e-mail da história.

Diante disso, pode-se concluir que a ideia principal era o armazenamento de informações, e além de possibilitar que pessoas de diferentes espaços físicos pudessem se relacionar. Com o passar do tempo, ocorreram as mudanças fundamentais para que a internet começasse a se transformar naquela que conhecemos hoje, quando foram criados os protocolos TCP/IP através de trabalhos experimentais realizados em conjunto pela ARPA e demais agências. Foi quando, no ano de 1983, formou-se a nomenclatura a qual usamos hoje em dia e a internet, então, começou a ser aquela que podemos encontrar atualmente.

No princípio o uso da internet era exclusivo dos Estados Unidos, depois chegou na Europa, em países como Holanda, Dinamarca e Suécia. Antigamente, a forma de estudo era

somente por meios de pesquisas em livros, isso demandava tempo, eram horas dentro de bibliotecas. Com a evolução da isso mudou, pois por meio dela, se abriram possibilidades de pesquisas, sejam elas acadêmicas ou para encontrar livros específicos. Além da extrema importância para a parte comercial, onde há possibilidades de comprar ou vender qualquer coisa, sem muito esforço, algo mais prático e simples, de rápida solução e sem ao menos sair de casa ou do local de trabalho.

Durante a década de 1990, a internet iniciou os primeiros esboços do que ela se tornaria nos dias de hoje, o cientista, professor e físico Tim Berners-Lee, criou um navegador ou browser como também é conhecido, a World Wide Web, o famoso “www” que antecede os sites de redes mundiais de Computadores. Houve, então, sua popularização pelo mundo com o surgimento de novos browsers, como a internet Explorer, Mozilla Firefox, Google Chrome, Opera, entre outros, e assim um aumento de usuários.

Perante isto, inicia-se a proliferação de sites, chats e das imensas redes sociais. Portanto iniciava um esboço do que se tornaria a internet, uma vigorosa ferramenta com navegadores/redes sociais que se tornaram indispensáveis no dia a dia das pessoas. Sabe-se que, com a chegada das redes sociais, a internet depreendeu um patamar de usabilidade e interação entre todo o mundo.

Em 1995, surgiu a Classmates, uma página que proporciona a troca de conhecimentos e uma forma de marcar encontros entre estudantes dos Estados Unidos e do Canadá, chegando a ter 50 milhões de usuários. Anos depois, em 2002, foi criado a fotolog, que conta com mais de 32 milhões de usuários em mais de 200 países, e seu objetivo é o compartilhamento de fotos.

Com o passar do tempo, as relações entre as pessoas ficaram mais rápidas. Principalmente com a chegada do e-mail, pois possibilitou as trocas de mensagens em tempos reais. As trocas de informações também ficaram mais acessíveis e facilitadas, devido ao surgimento e a expansão dos fóruns e debates online. Os sites então começaram a se modernizar, melhorando a qualidade dos conteúdos e da configuração das páginas, garantindo um fluxo maior do acesso de usuários. Por exemplo, o lançamento do GeoCities, lançado em 1994. Um serviço que oferecia ferramentas gratuitas para criação de páginas pessoais

eminentes pela localização do criador. Chegando a ter 38 milhões de usuários. Um ano após o serviço ter sido criado, surgiu em 1995, o The Globe, que era uma espécie de rede de blogs priscos, nele os usuários publicavam os conteúdos pessoais e compartilhavam as experiências do cotidiano, hobbies e outros assuntos de interesse.

Ainda em 1994, o Ward Cunningham criou o software WikiWikiWeb (na língua havaiana significa “web ágil”). Cunningham tinha como objetivo possibilitar que os usuários compartilhassem o processo de edição do próprio conteúdo usando um navegador de Internet. Em 1995, ele o adicionou ao website Portland Pattern Repository, um conjunto de padrões de projeto de software.

Em dezembro de 2006, Cunningham concedeu uma entrevista ao website Internet News.com, ele alegou que pensou patentear sua invenção, entretanto, após entender que para poder comercializá-la teria de sair e vender essa ideia e que improvavelmente alguém quisesse pagar por ela, então resolveu disponibilizá-la para sua comunidade, e para os desenvolvedores de software, pois segundo ele, representaria um cartão de apresentação e uma forma de ser reconhecido[1].

O website wiki, foi criado com a contribuição de Cunningham, é apelidado de wiki e configura-se por friccionar o trabalho anônimo, simplesmente por permitir que qualquer pessoa agregue conteúdo informacional e modifique as informações enviadas por outra pessoa e por proporcionar que todos os rascunhos de textos possam ser visualizados. Um exemplo relacionado a ele, é a enciclopédia multilíngue online Wikipédia. Totalmente sem fins lucrativos, gerenciado e operado pela Wikimedia Foundation desde janeiro de 2001. Ela é escrita voluntariamente por pessoas comuns com acesso à Internet de qualquer parte do mundo. São artigos com diversas informações, em todos os idiomas, são transcritos, modificados e ampliados por qualquer pessoa por meio dos navegadores como o Internet Explorer, Mozilla Firefox, Netscape, Opera, Safari, dentre outros programas que são capazes de ler páginas em HTML e as imagens. A Wikipédia chegou a registrar a existência de 515.407 verbetes em língua portuguesa, no ano de 2009, e no ano de 2010, 586 354.

[1] ARAYA , Elizabeth Roxana Mass; VIDOTTI , Silvana Aparecida Borsetti Gregório. **Criação, proteção e uso legal de informação em ambientes da World Wide Web**. São Paulo: Editora Unesp, 2010. 40-41 p. Disponível em: https://static.scielo.org/scielobooks/fdx3q/pdf/araya-9788579831157.pdf. Acesso em: 2 out. 2022.

O website BBCBrasil.com publicou um artigo em dezembro de 2005, com resultados de uma pesquisa realizada pela revista científica Nature, na qual apontava a Wikipédia como sendo tão precisa quanto a Enciclopédia Britânica, e destacou ter sido criticada devido às falhas de correção de seus verbetes. “A revista Nature examinou uma série de verbetes científicos nas duas fontes e encontrou poucas diferenças na precisão das definições. (BBC-Brasil.com, 2005, p.1).”[2] Após isso, o termo wiki, popularizou-se entre todos os internautas.

A internet é uma das tecnologias mais usadas diariamente pelas pessoas, qualquer atividade, seja pessoal ou profissional, é executada com todos os recursos e as ferramentas que são disponibilizadas nela. Com o passar do tempo, foram criadas as redes sociais, potencializando o uso da internet no mundo todo.

1.1 A chegada das redes sociais

Na década de 90, teve um outro marco histórico, que foi a chegada das redes sociais, elas elevaram o uso da internet a um novo escalão de usabilidade e interação entre milhões de usuários espalhados pelo mundo. Sendo as principais:

Em 1998, surgiu o Google, por meio dos estudantes da Universidade de Stanford, Larry Page e Sergey Brin, que escolheram dedicar o seu doutorado a uma condição de rastreamento da recém-criada World Wide Web. O trabalho dos jovens deu tão certo que na Califórnia, fundaram a Google Inc. Uma ideia de grande sucesso, que nasceu em garagens de teses, computadores e de um espírito empreendedor. Essa empresa importantíssima para os dias de hoje, nasceu com a ideia de facilitar a busca de informações em qualquer lugar do mundo.

[2] ARAYA , Elizabeth Roxana Mass; VIDOTTI , Silvana Aparecida Borsetti Gregório. **Criação, proteção e uso legal de informação em ambientes da World Wide Web**. São Paulo: Editora Unesp, 2010. 48 p. Disponível em: https://static.scielo.org/scielobooks/fdx3q/pdf/araya-9788579831157.pdf. Acesso em: 2 out. 2022.

Em 1995, o Classmates, uma página de interação para estudantes dos Estados Unidos e Canadá trocarem conhecimento ou marcar encontros. Chegou a ter mais de 50 milhões de usuários.

Em 2002 foi a vez do Fotolog, uma rede social para compartilhar fotografias. Os usuários publicavam atividades pessoais com pequenas descrições das suas rotinas, além da possibilidade de poder receber comentários e criar links para outros membros. Está ativa até então, e conta com mais de 32 milhões de usuários espalhados por 200 países.

Em 2003, surgiu o LinkedIn, uma rede social voltada para assuntos profissionais e vagas de emprego. Já o MySpace, é um blog feito para compartilhar conteúdos pessoais, fotos, vídeos e arquivos de áudio, dentre outros. Mutuamente com mais de 175 milhões e 25 milhões de usuários, as duas podem ser usadas diariamente.

Em 2004, foi marcante, pois deu início a popularidade das redes sociais. Surgindo o Orkut, do Google, e o Facebook. O Orkut[3] fez um sucesso espalhafatoso no Brasil, chegando a ser desativado. Foi criado pelo Mark Zuckerberg, após o desativamento o Facebook, assumiu esse posto em escala global e, hoje conta com 2,3 bilhões de usuários.

Em 2005, foi a vez do YouTube, lançado por três ex-funcionários do PayPal. Enfrentou dificuldades para decolar, no início, a plataforma chegou como uma solução definitiva para produzir, editar, compartilhar e consumir conteúdos em vídeo. Hoje tem mais de 1 bilhão de usuários.

Em 2006, chegou o Twitter, uma rede social diferenciada, ele padronizou um estilo de microblogs para compartilhamento de conteúdos de forma mais ágil e sucinta com um limite bem baixo de até 140 caracteres por postagem. Em 2017, esse número foi aumentado para 280 caracteres. Atualmente, a rede conta com mais de 326 milhões de usuários ativos.

[3] PETRIN, Natália. Redes Sociais. **Todo Estudo**. Disponível em: https://www.todoestudo.com.br/historia/redes-sociais. Acesso em: 08 de December de 2022.

Em 2009, o WhatsApp foi criado, ele é um aplicativo multiplataforma de mensagens instantâneas e chamadas de voz para smartphones. Além de mensagens de texto, os usuários podem enviar imagens, vídeos e documentos em PDF/ Word, além de fazer ligações grátis por meio de uma conexão com a internet, seu recorde foi quando em setembro de 2015, o aplicativo alcançou a marca dos 900 milhões de usuários ativos e esse número vem crescendo absurdamente.

Em 2010, o Instagram foi lançado. A rede é uma criação conjunta dos engenheiros de software norte-americano Kevin Systrom e o brasileiro Mike Krieger. Especialmente para postagens de fotografias, conta com vários filtros interativos, mecanismos para a interação e mais de 1 bilhão de usuários. É a segunda maior rede social do mundo.

Em 2011, surgiu o Google +, uma rede social criada. Entretanto, ela não chega a ter tanta expressão em número de usuários, possuindo um total de 400 milhões de usuários inscritos, nos quais 100 milhões participam diariamente.

Outras duas redes sociais que precisam ser mencionadas pelo seu grande número de acessos são Snapchat e Tik Tok[4]. A primeira completou 10 anos em 2021 com mais de 265 milhões de usuários. O TikTok, por outro lado, está presente em 150 países e tem mais de 1,23 bilhão de usuários ao redor do mundo. Ambos focam em vídeos, não em fotos, e na pandemia que ocorreu em 2020, o número de usuários cresceu.

1.2 A Internet no Brasil

É notório que a tecnologia, a priori, é criada em países mais desenvolvidos e, após isso, é espalhada para os demais países, alcançando o mundo. Já no Brasil, a internet chegou justamente na década de 80. Essa chegada se deu 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 de Computação Científica), as universidades brasileiras moveram-se para manter o compartilhamento de informações com os Estados

[4] VOLPATO, Bruno. **Ranking**: as redes sociais mais usadas no Brasil e no mundo em 2022, com insights e materiais. [*S. l.*], 23 maio 2022. Disponível em: https://resultadosdigitais.com.br/marketing/redes-sociais-mais-usadas-no-brasil/. Acesso em: 2 out. 2022.

Unidos. A LNCC foi a primeira a conseguir acesso à bitnet, no mês de setembro de 1988, mediante uma conexão com o FERMILAB (Fermi National Accelerator Laboratory) em Chicago. Então a FAPESP criou a rede ANSP (Academic Network at São Paulo), que relacionava a Universidade de São Paulo, a Universidade de Campinas, a Universidade Estadual Paulista e o Instituto de Pesquisas Tecnológicas do Estado de São Paulo. Com o passar do tempo, essas informações chegaram até a Universidade Federal do Rio Grande do Sul, e assim foi se estendendo para as demais universidades.

No Brasil, a internet veio, primeiramente, para ser utilizada no âmbito acadêmico, iniciando nas universidades em São Paulo e usando essa rede para se comunicar com as demais universidades em outros lugares do mundo. O IBASE (Instituto Brasileiro de Análises Sociais e Econômicas), fundado em 1981, teve como seus objetivos propagar as informações à sociedade civil, incluindo a democratização do acesso às redes de computadores no país, através de um projeto internacional chamado Interdoc, bem no meio da década de 80. Entretanto, esse projeto estava custando um valor muito alto, sendo necessário então buscar meios alternativos para ser possível essa conexão internacional, com custos menores.

Como citado anteriormente, o projeto era somente para uso no meio acadêmico, porém, examinaram-se formas de amplificar o uso para as demais atividades, chegando ao alternex, é um serviço internacional de mensagens e conferências eletrônicas pioneiro no país. Graças ao alternex, conseguiu-se realizar a troca de mensagens com vários sistemas de correio eletrônico do mundo todo, incluindo a internet. O alternex foi o primeiro serviço brasileiro de acesso à internet fora do âmbito acadêmico.

No final do ano de 1994, o governo brasileiro passou a expandir investimentos na nova tecnologia, por meio do Ministério de Ciência e Tecnologia e do Ministério das Comunicações. A Embratel e a RNP foram responsáveis pela criação da estrutura necessária para exploração comercial da internet. A Embratel começou seu serviço de acesso à internet de modo experimental, escolhendo 5 mil usuários para testar o serviço. Em maio de 1995, o acesso à internet através da Embratel começou a 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. Entretanto, o que era um serviço muito limitado, iniciaria o seu “sucesso” inicialmente no ano de 1996, quando recebeu melhorias, crescente número de

usuários, e o acesso em todo território nacional amplificou-se por meio das redes locais de conexão.

Nos dados divulgados pelo Ministério da Ciência e Tecnologia em 2011, verificou-se que aproximadamente 80% da população teve acesso à internet, correspondendo, portanto, a 60 milhões de computadores em uso. Independentemente da internet ter tomado enormes proporções apenas na década de 90, o Brasil, entretanto, passou a ser um dos países que mais utiliza essa ferramenta, tornando-se o quarto país com mais usuários, atrás apenas de países como China, índia e Estados Unidos, países estes que possuem uma população ilimitada em comparação com o nosso. Porém, através disso, podemos vislumbrar o quanto a população se tornou dependente, e que talvez não queiram, nem possam viver sem ela. Sabe-se que é uma ferramenta que nos ajuda, entretém e auxilia, mas o seu uso descontrolado tem tornado tudo cada vez mais difícil, às vezes até fora de controle o acesso e a forma como muitos utilizam, existem aqueles que usam suas habilidades, talentos e conhecimentos para o bem, há também os que usam para tirar proveito das situações, aplicar golpes, dentre outras formas ruins, e assim, surgem, portanto, os crimes no mundo virtual, os quais serão abordados no próximo capítulo.

É de conhecimento mundial, que as novas tecnologias de informação e de comunicação abrem grandes perspectivas à sociedade do futuro. A informação, quando produzida, circula instantaneamente, pode ser recebida, tratada, incorporada em esquemas lógicos, científicos, transformada por cada um de nós em conhecimento pessoal, acréscimo de compreensão, sabedoria, em valor acrescentado para o mercado ou a sociedade.

Nos dias de hoje, a Internet possibilita uma amplificação rápida, por meio das novas tecnologias de informação. O conhecimento gerado permite que as empresas melhorem a sua eficiência, além de oferecerem novos produtos e serviços pelos quais seus consumidores, por meio dos mecanismos de mercado, manifestem suas preferências. Com o avanço da internet, é gerada uma união entre as fontes de informação em bibliotecas, em documentos e arquivos, são realizadas pesquisas em bases de dados, em linguagem natural ou controlada. O livre acesso a dissertações, actas de congressos, comunicações e relatórios, enciclopédias e dicionários digitais.

A priori, a Internet foi criada para fins acadêmicos, como explicado no início desse primeiro capítulo. Porém, nos dias de hoje, ela serve para tudo: e-commerce, comunicação, entretenimento de todo o tipo, assistir séries, filmes, jogar. Reencontrar pessoas do passado. Usufruir das redes sociais, ter acesso a jornais e revistas. Além de possibilitar saber a previsão do tempo. E outras tantas possibilidades infinitas.

Além dos benefícios acadêmicos e das redes sociais, a internet abrange tantas informações, que acaba sendo um mecanismo de enciclopédia mundial, a facilidade em realizar comprar de maneira prática, diversas atividades de lazer, infinitas informações, usar Internet Banking, realizar transferências bancárias, que juntamente com a internet vendo abrindo novas opções fornecidas pelos aplicativos do banco, como por exemplo o pix, um método de transferência sem cobranças de taxas, diminuição de distâncias, a busca de empregos em sites, na verdade se tornando uma quebra de fronteiras, principalmente no meio educacional.

A forma como a internet melhorou o acesso à educação é notória, como por exemplo, o caso da University of People[5], que tem por objetivo principal levar educação de nível superior a locais de difícil acesso. Ela oferece cursos de graduação em formato EAD (Educação à Distância) de graça, o interessado em fazer só paga para realizar as provas. A University of People[6] é uma boa opção para quem não pode perder tempo ou não tem condições de arcar com os gastos em passagens pelos deslocamentos e quer ajustar seus horários para estudar em casa. Um outro exemplo dessa melhora são as Ferramentas para apoio escolar de crianças e adolescentes com fontes diferentes e divertidas para aprendizado mais interativo. Principalmente para aqueles que possuem alguma deficiência ou dificuldade de aprendizado.

---

[5] FORBES. *In*: HIGH, Peter. **A Conversation With The President Of The World's First Non-Profit, Tuition-Free, Accredited, Online University**. [*S. l.*], 3 mar. 2014. Disponível em: https://www.forbes.com/sites/peterhigh/2014/03/03/a-conversation-with-the-president-of-worlds-first-non-pro%EF%AC%81t-tuition-free-accredited-online-university/?sh=305ecdf45c7d. Acesso em: 2 out. 2022.

[6] LEWIN, Tamar. **Israeli Entrepreneur Plans a Free Global University That Will Be Online Only**. [*S. l.*], 25 jan. 2009. Disponível em: https://www.nytimes.com/2009/01/26/education/26university.html#:~:text=An%20Israeli%20entrepreneur%20with%20decades,the%20University%20of%20the%20People. Acesso em: 2 out. 2022.

1.2.1 Economia

A Internet possibilita diversas atividades econômicas que não seriam possíveis pela forma tradicional, dentre elas, O Ecommerce, as Plataformas de Streaming, empresas totalmente online, assim como Portais, e mercados totalmente novos como a carreira de Digital Influencer, que além de ser uma carreira muito lucrativa, qualquer pessoa de qualquer idade pode seguir, e mediante ao sucesso nessa profissão, acabar gerando empregos novos e muita visibilidade para as empresas que contratarem seus serviços. Inegavelmente é uma profissão que não existia há um século atrás.

Além disso, devido aos serviços digitais dos bancos “o Internet Banking”, possibilitou pagar um boleto de forma fácil. Não há mais a necessidade de se deslocar a uma Agência Bancária ou Lotérica, enfrentar filas, aguardar e então pagar no caixa. Ao invés disso, basta pagar de casa sem esforço e sem burocracias.

A busca por emprego através de sites é cada vez mais comum. Como citado anteriormente, o LinkedIn é uma rede social para uso corporativo, conseguir emprego e se socializar profissionalmente. Existem vários outros sites em que os interessados cadastram suas vagas em aberto e os candidatos podem se inscrever. Por exemplo InfoJobs, Indeed, Trabalha Brasil, Vagas.com e Emprega Brasil.

1.2.2 Informação e Responsabilidade

É tudo novo para as gerações que estão passando por essa transição. Jovens e adolescentes que iniciam desde cedo o uso dos celulares, eles muitas das vezes, não são maduros o suficiente para lidar com críticas, e isso acaba gerando problemas, sejam psicológicos ou com a própria saúde do corpo. Há pessoas com certas características que dificultam a socialização, como por exemplo a timidez, e podem se sentir mais confiantes ao usar plataformas online. Finalmente poder fazer amigos e discutir temas de seu interesse. Para

quem sabe usar a internet, os benefícios são inúmeros, entretanto, alguns devem ser observados, afinal, nem tudo que você lê, vê ou ouve deve ser considerado real.

É importante lembrar que a internet é um canal democrático onde as pessoas podem postar o que lhes interessa, mas nem sempre isso é verdadeiro e honesto, muitas pessoas usam a internet para prejudicar outras pessoas. Mesmo com algumas desvantagens, a Internet é, sem dúvida, o canal de informação mais democrático e incrível do planeta, oferecendo aos seus usuários: o acesso à informação nunca foi tão difundido e imediato como hoje.

1.2.3 Acessibilidade

O acesso à informação nunca foi tão amplo e instantâneo como atualmente. Um dos grandes benefícios da internet é possibilitar que as informações estejam à sua disposição sempre, e nos mais diversos modelos de mídias, como por exemplo: notícias jornalísticas, reportagens, filmes, documentários, dentre outros. A maior parte desses conteúdos estão disponíveis gratuitamente, onde qualquer assunto pode ser encontrado, sendo necessário apenas procurar em um site de busca e acessar os mais diversos materiais de todas as partes do mundo.

1.2.4 Praticidade

Com a internet a vida fica mais fácil e prática, pois é possível através dela: pesquisar preços, fazer compras, planejar viagens, realizar reuniões, participar de aulas, sejam ao vivo ou gravadas, estudar literalmente sobre qualquer coisa, trabalhar em Home Office. Atualmente, milhões de pessoas no Brasil não precisam mais se dirigir a alguma empresa para desenvolver as suas atividades profissionais, porque o home office, através da internet, é uma realidade. O Instituto de Pesquisa Econômica Aplicada (Ipea)[7] divulgou um estudo, em julho de 2021, informando que 11% dos trabalhadores ativos no Brasil exercem suas profissões remotamente, e isso foi um grande avanço que ocorreu nos meios trabalhistas.

[7] AGÊNCIA BRASIL. *In*: CAMARGO, Marcelo. **Ipea**: 11% dos trabalhadores fizeram home office ao longo de 2020. Rio de Janeiro, 15 jul. 2021. Disponível em: https://agenciabrasil.ebc.com.br/economia/noticia/2021-07/ipea-11-dos-trabalhadores-fizeram-home-office-ao-longo-de-2020. Acesso em: 2 out. 2022.

1.2.5 Entretenimento

O entretenimento também é encontrado na internet, ele oferece lazer para toda a família, no entanto, é importante ficar atento ao que as crianças e adolescentes estão acessando na rede mundial, pois como já mencionado, ela é democrática e aceita conteúdos não recomendáveis para essa fase de desenvolvimento e descobrimento do mundo. A internet possibilita que você tenha acesso a: jogos, shows, espetáculos, esportes, filmes, músicas, conteúdos sobre o seu hobby preferido. Porém existem os malefícios da internet, explicados no próximo tópico.

1.3 Os Malefícios da Internet

Apesar da internet ser um meio com diversas vantagens, existe o lado negativo da mesma, como por exemplo: Os Crimes virtuais[8], o uso inapropriado que acaba gerando vícios, o isolamento, a falta de interação social, viver mais a vida online do que a offline. Quanto ao objetivo principal que motivou a pesquisa, são os crimes virtuais, que estão crescendo absurdamente, envolvendo assim os governos, pois estão buscando se esforçar para criar leis que atendam a esse contexto negativamente novo da sociedade.

A internet não é uma terra sem lei como muitos podem idealizar. No Brasil, já existe o Marco Civil[9] da Internet, que possibilita a apresentação dos direitos, deveres e regras para proteção dos usuários. Nos dias de hoje, é necessário estar atento para não cair em golpes e acabar se tornando vítima de cybercriminosos. Buscar uma forma segura para evitar esse mal. Se durante o uso da internet ocorrer dúvidas sobre a confiabilidade de uma página ou aplicativo acessado, o recomendado é não clicar e não usar. Antes de tudo buscar informações e ser prudente. Com o avanço da internet é cada vez mais comum a aparição de páginas falsas,

---

[8] PSICANALISE CLÍNICA. **Conhecendo os Benefícios e Malefícios da Internet**. [*S. l.*], 3 jan. 2020. Disponível em: https://www.psicanaliseclinica.com/beneficios-e-maleficios-da-internet/. Acesso em: 2 out. 2022.

[9] ABRAMOVAY, Pedro. **O Marco Civil e a Política dos Netos.** [S. l.], 7 maio 2014. Disponível em: https://sul21.com.br/opiniao/2014/05/o-marco-civil-e-a-politica-dos-netos-por-pedro-abramovay/. Acesso em: 2 out. 2022.

com o objetivo de roubar dados. Além dos mais comuns [10]perigos, como os Vírus, Spams e E-mails maliciosos.

Há especialistas que apontam os mais possíveis riscos que estamos expostos na internet. A busca por “aceitação” acaba gerando uma exposição excessiva motivados por “likes”, postar qualquer coisa para conseguir mais visualizações tem se tornado uma prática comum. E caso esse objetivo não seja alcançado, as pessoas se sentem frustradas. Por esse motivo, aparecem pessoas que se utilizam do anonimato de um perfil para causar todo tipo de discórdia e propagar o ódio. Tudo isso cria um ambiente hostil psicologicamente. O vício na internet também é utilizado como “forma de escape” entre pessoas que preferem usar a internet ao convívio social.

1.4 Hacker o surgimento

Hackers[11] são aqueles que trabalham para resolver problemas e criar soluções envolvendo tecnologia, computação e computação, desenvolvendo e modificando software e hardware de computador, não necessariamente para fins de crime. Eles também desenvolvem novos recursos sobre sistemas de computador.

As origens do termo hacker remontam aos Estados Unidos na década de 1960. Começa usando a palavra "hack" para designar uma solução inovadora para qualquer problema. Ao longo dos anos, o termo foi associado a programadores de computador que eram renomados na época no Massachusetts Institute of Technology (MIT) e no resto do mundo. Eles combinam conhecimento computacional específico com instintos criativos. Embora os hackers tenham surgido nos Estados Unidos, eles acabaram se tornando um fenômeno global e podiam ser encontrados em qualquer lugar do mundo. Há lugares como Paquistão e Índia.

Os hackers possuem um mercado muito amplo para atuarem, principalmente para aqueles que optam em dedicar-se a sistemas de segurança de informação. Como tudo hoje é

[10] RIBEIRO, Paulo. **Benefícios e Malefícios da Internet**. [*S. l.*]. Disponível em: http://efaa1.weebly.com/internet---benefiacutecios-e-maleficios.html. Acesso em: 2 out. 2022.

[11] CAETANO, Érica. **O que é hacker?**; Brasil Escola. Disponível em: https://brasilescola.uol.com.br/informatica/o-que-e-hacker.htm. Acesso em 31 de outubro de 2022.

feito pela internet, de uma simples realização de compras a operações financeiras com criptomoedas, essa área expandiu-se muito para aqueles que detêm o conhecimento em programação.

Um hacker pode atuar diretamente em setores ligados à perícia forense, pesquisas de vulnerabilidade, engenharia de projetos, desenvolvimento de softwares, testes de invasão, gestão de riscos, dentre outros. Um hacker ganha muito dinheiro com os pagamentos feitos por empresas que lançam alguns desafios para terem seus sistemas invadidos e, com isso, desenvolverem melhorias na sua segurança.

1.4.1 Hacker x Cracker

Considerando que os hackers não cometem crimes virtuais, a expressão certa para se usar para aqueles que cometem, na verdade, o termo "cracker"[12]. Pode-se definir os crackers como hackers que usam o conhecimento adquirido em informática, computação e demais tecnologias para invadir ilegalmente os sistemas, sites, servidores, bancos de dado, dentre outros. Alguns casos, o objetivo é apenas testar a vulnerabilidade dos serviços, porém em outros, é específico para obter algum ganho financeiro ou pessoal. Portanto, o cracker trata-se daquele que consegue invadir os sistemas de segurança operacional com o simples objetivo de ter proveito pessoal, como por exemplo, modificar um programa para que ele não precise mais ser pago, jogando vírus na rede, clonando dados e roubando senhas. Então, podemos falar que o cracker seria um "hacker do mal". A expressão foi criada em 1995, justamente para distingui-los daqueles que seriam os "hackers do bem".

Mediante a isto, com todo o avanço da tecnologia, podemos perceber que além das melhorias positivas, uma pessoa ou um grupo de pessoas, utilizam desse "bem" de uma forma negativa, trazendo muitos malefícios, danos psicológicos e até cometendo crimes, que serão explicados no próximo capítulo.

---

[12] AMARIZ, Luiz Carlos. Infoescola. **Hackers e Crackers**. [*S. l.*]. Disponível em: https://www.infoescola.com/informatica/hackers-e-crackers/. Acesso em: 25 out. 2022.

2. O CRIME CIBERNÉTICO

O crime cibernético se classifica como uma atividade criminosa, cujo objetivo principal é danificar os computadores e as redes por outros motivos que não envolve o lucro, ou simplesmente por "maldade". Em alguns casos os motivos são pessoais ou políticos. O crime cibernético é realizado por indivíduos ou organizações. Alguns cibercriminosos são organizados, e extremamente perigosos, pois utilizam técnicas avançadas e são altamente capacitados com os termos técnicos. Já outros são hackers amadores, utilizam um computador, alguma rede de computadores ou um dispositivo conectado à rede. A maioria dos crimes cibernéticos é cometida por esses grupos de cibercriminosos e hackers que visam ganhar dinheiro a qualquer custo. O docente Rossini definiu os crimes virtuais como:

> O conceito de "delito informático" poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informação em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade a confidencialidade.[13]

Outro docente, o Pinheiro definiu como:

> Os crimes digitais podem ser conceituados como sendo as condutas de acesso não autorizado a sistemas informáticos, ações destrutivas nesses sistemas a interceptação de comunicações, modificações de dados, infrações a direitos de autor, incitação ao ódio e descriminação, escárnio religioso, difusão de pornografia infantil, terrorismo entre outro.[14]

Alguns exemplos dos tipos de crimes cibernéticos, são: Fraude por e-mail e pela Internet, fraude de identidades (onde informações pessoais são roubadas e usadas), roubo de dados financeiros ou de pagamento com cartão, roubo e venda de dados corporativos. Além disso, também o Ciber Extração (exigir dinheiro para evitar um ataque ameaçado). Ataques de ransomware (um tipo de ciber extrusteio). Crypto Jacking (onde hackers exploram criptomoedas usando recursos que não possuem). Espionagem cibernética (onde hackers acessam dados do governo ou de uma empresa), interferência em sistemas de modo a

[13] ROSSINI, Augusto Eduardo de Souza. Informática, telemática e direito penal. p. 110. São Paulo: Memória Jurídica, 2004.
[14] PINHEIRO, Patrícia Peck. Direito Digital. p. 46. 4. Ed. São Paulo: Saraiva, 2010.

comprometer uma rede, violação de direitos autorais, jogos de azar ilegais. venda de itens ilegais online, Incitação, produção ou posse de pornografia infantil, dentre outros.

Os crimes cibernéticos envolvem um dos seguintes itens ou ambos: Atividade criminosa direcionada a computadores usando vírus e outros tipos de malware. Atividade criminosa que usa computadores para cometer outros crimes.

Os cibercriminosos visam computadores para poderem infectá-los com malware para danificar todos os dispositivos ou simplesmente impedi-los de funcionar. Eles utilizam o malware para excluir ou roubar dados. Ou simplesmente podem impedir que os usuários utilizem um site, rede ou impedir que uma empresa forneça um serviço de software a seus clientes, o que é chamado de ataque de negação de serviço (DoS). Existe também a possibilidade de envolver o uso de computadores ou redes para disseminar malwares, informações ou imagens ilegais.

Os cibercriminosos estão frequentemente fazendo as duas coisas ao mesmo tempo. O ataque pode ocorrer com computadores, colocando vírus e, após isso, espalham o malware em outros computadores ou por toda a rede. Algumas jurisdições reconhecem uma terceira categoria de crime cibernético, que é onde um computador é usado como acessório para o crime. Um exemplo disso é o uso de um computador para armazenar dados roubados.

Alguns exemplos famosos encontrados no Kaspersky de diferentes tipos de ataques criminosos cibernéticos usados por cibercriminosos.

Os Ataques de malware:

> O ataque de malware acontece por meio de um sistema ou por uma rede de computadores que são infectados por um vírus de computador ou outro tipo de malware. Um computador corrompido por malware pode ser usado por criminosos cibernéticos para vários fins. Alguns deles roubam dados confidenciais, usam o computador para realizar outros atos criminosos ou causar danos aos dados.
> Um exemplo famoso de ataque de malware foi o ataque do ransomware WannaCry, um crime cibernético global cometido em maio de 2017. O WannaCry é um tipo de ransomware, um malware usado para extorquir dinheiro, pois mantém os dados ou o dispositivo da vítima como refém em troca de um resgate. O ransomware visava uma vulnerabilidade em computadores que executam o Microsoft Windows.
> Quando o ataque do ransomware WannaCry aconteceu, 230.000 computadores foram afetados em 150 países. Os usuários ficaram sem acesso aos próprios arquivos

e receberam uma mensagem exigindo o pagamento de um resgate em Bitcoins para terem o acesso de volta. A priori, pode-se dizer que no mundo todo, o crime cibernético do WannaCry tenha causado US$ 4 bilhões em perdas financeiras. Nos dias de hoje, esse ataque se destaca por sua dimensão e impacto.[15]

Os Ataques DoS distribuído:

Um dos ataques famosos, são os ataques de DoS distribuído (DDoS), é um tipo de ataque cibernético que os cibercriminosos utilizam para paralisar um sistema ou uma rede. Algumas vezes, são usados dispositivos conectados na Internet das Coisas (IoT) usados para iniciar os ataques de DDoS. É um ataque que sobrecarrega um sistema recorrendo a um dos protocolos de comunicação padrão que ele usa para enviar solicitações de conexão por spam ao sistema. Os criminosos cibernéticos que fazem extorsões cibernéticas podem usar a ameaça de um ataque DDoS com o objetivo de extorquir dinheiro. O DDoS pode ser utilizado como uma tática para distração enquanto ocorre outro tipo de crime cibernético. Por exemplo, o ataque DDoS de 2017 a um site da loteria nacional do Reino Unido. Ele paralisou o site e o aplicativo móvel da loteria, impedindo que os cidadãos do Reino Unido jogassem. O motivo da ocorrência do ataque permanece desconhecido. Existe uma possibilidade de que o ataque tenha acontecido por uma tentativa de chantagear a loteria nacional.[16]

O Phishing:

O termo inglês “fishing”, significa “pescar”. O phishing é uma tentativa de atrair usuários por meio de links, e-mails, aplicativos ou sites criados, com o objetivo de roubar dados, as senhas, números de telefone e de cartões. Na maioria das vezes, os criminosos fingem por meio de fakes, ser alguém conhecido e confiável ou mesmo alguma empresa que tenha boa reputação a fim de atrair vítimas. Esse termo foi criado no princípio da internet, ocorreu na segunda metade dos anos 1990, quando os hackers tinham o objetivo de atrair usuários para roubar suas contas hospedadas no America Online (AOL). O Brasil é um dos países que lideram os ataques: Ele ficou em quinto lugar na lista, atrás apenas de Venezuela, Portugal, Tunísia e França.[17]

---

[15] KASPERSKY. **O que são crimes cibernéticos?**: Como se proteger dos crimes cibernéticos?. [*S. l.*]. Disponível em: https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime. Acesso em: 25 out. 2022.

[16] KASPERSKY. **O que são crimes cibernéticos?**: Como se proteger dos crimes cibernéticos?. [*S. l.*]. Disponível em: https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime. Acesso em: 25 out. 2022.

[17] KASPERSKY. **O que são crimes cibernéticos?**: Como se proteger dos crimes cibernéticos?. [*S. l.*]. Disponível em: https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime. Acesso em: 25 out. 2022.

O Kits De Exploits:

> Uma ferramenta extremamente perversa, e que na maioria das vezes pode ser imperceptível aos olhos dos navegadores na internet. Os criminosos utilizam os kits de exploits (coleções de explorações) como forma de aproveitamento das falhas e bugs que acontecem com nos computadores. Softwares adquiridos por meios clandestinos que possibilitam a instalação até por sites confiáveis. Um HTML invisível, eles fazem com que as vítimas não notem que há algo errado. Quando um determinado usuário clica no programa, esse kit vai diretamente em busca dos softwares que estão vulneráveis no computador. Por exemplo, por meio de um browser (navegador) que está desatualizado ou está com uma versão antiga, devido a isso o criminoso consegue observar a navegação da vítima e, assim, consegue roubar dados e informações guardados no computador, seja ele pessoal ou de uma empresa.[18]

O Ransomware:

> Ransomware é um malware, uma série de vírus que podem acessar, inspecionar e bloquear computadores, causando uma tremenda confusão para os usuários. A maneira mais comum que os criminosos usam o ransomware é para ameaçar as vítimas com um resgate depois de instalá-lo e bloquear o acesso a um computador. Principalmente por motivos financeiros. O ransomware também se esconde em softwares carregados de vírus que as vítimas podem acessar por meio de mensagens ou vários sites. Sem a proteção adequada, o risco é alto, pois você não poderá mais acessar seus próprios dados a partir de blocos pré-especificados. [19]

O Bullying Virtual:

> O cyber bullying ou cyberbullying é uma extensão do que acontece em muitas áreas da vida real, ou seja, o bullying que ocorre na escola, no trabalho, na faculdade ou onde se convive com a sociedade. A única diferença é que o contato entre a vítima e o agressor não é presencial, é somente online. Pode acontecer por e-mail, em fóruns de discussões, redes sociais e websites, embora seja possível que ocorra em vários ambientes virtuais, o foco principal é nas redes sociais, lá onde a facilidade das mensagens acabam se tornando ofensas e ameaças dos criminosos.[20]

---

[18] KASPERSKY. **O que são crimes cibernéticos?**: Como se proteger dos crimes cibernéticos?. [*S. l.*]. Disponível em: https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime. Acesso em: 25 out. 2022.

[19] KASPERSKY. **O que são crimes cibernéticos?**: Como se proteger dos crimes cibernéticos?. [*S. l.*]. Disponível em: https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime. Acesso em: 25 out. 2022.

[20] KASPERSKY. **O que são crimes cibernéticos?**: Como se proteger dos crimes cibernéticos?. [*S. l.*]. Disponível em: https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime. Acesso em: 25 out. 2022.

A Fake News:

> Às Fake News significam “notícias falsas” que são publicadas em redes sociais e meios de comunicação como se fossem informações verídicas. Essa forma de "notícia” na maioria das vezes é divulgada com o objetivo de prejudicar uma pessoa ou grupo de pessoas, normalmente as figuras públicas, entretanto é algo que pode ser realizado com o objetivo de atingir qualquer pessoa. As Fake News espalham-se velozmente, são informações falsas que apelam para o emocional do leitor/espectador, atingindo assim o seu objetivo, as pessoas que recebem esse tipo de notícia, muita das vezes não buscam pesquisar se realmente é verdade apenas repassam sem medir as consequências desse ato. [21]

Em 2016, o termo “Fake News” obteve uma força mundial, devido à corrida presidencial nos Estados Unidos, nessa época os conteúdos falsos que se espalharam sobre a candidata Hillary Clinton foram compartilhados por meio impetuoso pelos eleitores de Donald Trump. Quando as Fakes News entram no âmbito virtual por meio das redes sociais, acontecem então a criação de perfis falsos com fotos “tiradas” da internet se passando por alguém ou uma figura pública, os dados pessoais e publicações diárias, entre outros, Após isso, esses perfis começam a espalhar as notícias falsas por meio de vídeos com montagens falsas, além de incentivar as pessoas a fazerem o mesmo.

A divulgação das notícias falsas gera várias consequências, pois é um ato muito perigoso, quem compartilha essas notícias está assumindo a responsabilidade de colocar a vida de outra pessoa ou de um grupo de pessoas em risco. Realizar montagens com fotos e vídeos manipulados acabam trazendo riscos de forma geral, além de está incentivando o preconceito e nos casos mais graves resultando em mortes. Um exemplo da consequência: quando ocorre um linchamento de inocentes

Em 2014, o Brasil presenciou o caso de uma Fake News envolvendo uma mulher chamada Fabiane Maria de Jesus, uma mulher casada mãe de dois filhos que infelizmente teve um fim trágico, ela foi confundida com uma suposta “sequestradora de crianças”. Após ser linchada. Conforme foi divulgado pela Polícia Civil, a foto ligada equivocadamente à dona de casa era de 2012. Tratava-se de uma mulher acusada de tentar roubar um bebê no Rio de Janeiro. Sem qualquer ligação com o local que ocorreu essa fatalidade. Após todo esse

[21] KASPERSKY. **O que são crimes cibernéticos?**: Como se proteger dos crimes cibernéticos?. [*S. l.*]. Disponível em: https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime. Acesso em: 25 out. 2022.

linchamento, a Fabiane foi arrastada até uma passarela e lá foi encontrada e socorrida por policiais militares, entretanto, faleceu dois dias depois.

2.1 Impacto dos crimes cibernéticos

É de conhecimento geral, que o crime cibernético está crescendo absurdamente, conforme o relatório Estado da resiliência da segurança cibernética de 2021 da Accenture, “os ataques de segurança tiveram um aumento de 31% de 2020 a 2021.”[22] Ano a ano, o número de ataques por empresa aumentou de 206 para 270.

Todos os ataques a empresas afetam os indivíduos, pois a maioria armazena dados confidenciais e informações pessoais de seus clientes. Basta apenas um ataque, seja ele qual for, de uma violação de dados, malware, ransomware ou ataque DDoS, e isso gera nas empresas de todos os portes uma média de US$ 200.000, e muitas empresas afetadas fecham as portas dentro de meses após o ataque, de acordo com a seguradora Hiscox. A Javelin Strategy & Research publicou o Identity Fraud Study (Estudo sobre fraude de identidade) em 2021, que constatou que as perdas por fraude de identidade no ano totalizaram US$ 56 bilhões[23].

Para ambos os envolvidos o impacto dos crimes cibernéticos pode ser profundo, a ponto de acarretar prejuízo e danos financeiros, e por consequência a perda de confiança e danos à reputação de alguém ou até mesmo da empresa. Mediante a esses meios, os infratores podem roubar informações e dados confidenciais, aplicando golpes como os de falsidade ideológica. Portanto, esses crimes envolvem, de um lado um ou mais criminosos e do outro uma ou mais vítimas. Devido à evolução dos dispositivos nas últimas décadas, houve uma evolução da forma como os delitos são cometidos, ou seja, qualquer pessoa está sujeita a ser atacada.

---

[22] ACCENTURE**. The state of cybersecurity resilience 2021.** [*S. l.*], 3 nov. 2021. Disponível em: https://www.accenture.com/pt-pt/insights/security/invest-cyber-resilience. Acesso em: 25 out. 2022.

[23] FINTECHS. **Relatório**: O estudo de fraude de identidade de 2021. [*S. l.*], 7 abr. 2021. Disponível em: https://fintechs.com.br/relatorio-o-estudo-de-fraude-de-identidade-de-2021/. Acesso em: 25 out. 2022.

2.2 A lei no Brasil contra crimes cibernéticos

No ano de 2012 surgiu no Brasil uma legislação voltada para os crimes cibernéticos, conhecida como a Lei Carolina Dieckmann, que é uma atriz que teve 36 fotos íntimas vazadas na internet, a Lei Nº 12.737/2012 foi adicionada no Código Penal passando a tipificar delitos em ambientes virtuais. O caso que ocorreu com a atriz gerou uma grande repercussão, entretanto, no país já exigia esse tipo de legislação devido um alto número de golpes e roubos de senhas que aconteciam na internet, nos dias de hoje mais ainda, pois esse número vem aumentando absurdamente.

Os criminosos invadem dispositivos de informática, como computadores, notebooks, celulares, tablets e entre outros, alimentam programas que violam dados e, assim, os expõem a negociarem ou transmitirem essas informações, e isto deve ser penalizado. As sanções para os que praticam e buscam obter informações de maneira ilícita, vale tanto para quem comete o crime de forma online ou offline. As penas são de três meses a até dois anos de prisão, além de multas. Devido ao crescente número de casos, o estado iniciou a implementação de delegacias especializadas.

Um breve resumo da forma como o chamado Marco Civil da Internet, de 2014 (Lei Nº 12.965/2014), estipula e regula direitos e deveres dos internautas, com a intenção de proteger informações pessoais e dados privados dos usuários, ou seja, ocorrem as medidas judiciais contra os crimes online e relacionadas a possíveis retiradas de conteúdos ofensivos ou criminosos da rede. Existem três categorias de crimes cibernéticos. O primeiro são os ataques que utilizam especificamente os computadores. O segundo são aqueles que buscam um acesso a outros computadores ou dispositivos, por meio da obtenção ilícita de uma determinada rede. E o terceiro são os crimes nos quais o computador não executa a sua principal função, porém é fundamental para armazenar, por exemplo, documentos confidenciais obtidos a partir de acessos ilegais.

As três categorias levam os criminosos a arrancarem dinheiro das vítimas, inclusive por meio da exigência de criptomoedas em troca dos dados adquiridos ilegalmente. Isso tudo é muito bem planejado com o objetivo de mexer no psicológico das vítimas, para que ocorra o impacto financeiro tanto para elas quanto para empresas ou instituições. As

vítimas acabam tendo que arcar com custos de tratamento psicológico e psiquiátrico. Afinal, os criminosos ameaçam, realizam o sequestro de dados e extorsões que geram um clima de terror para os que sofrem o golpe. Para as empresas e organizações, o impacto também é grande, porém mais voltado para a parte financeira. Um estudo, feito pela McAfee, demonstrou que o custo das práticas criminosas online é de mais de 1% da produção econômica mundial. Alguns exemplos desses crimes:

Furto qualificado: A lei acrescentou ao Código Penal o agravante do furto qualificado por meio eletrônico que aconteça com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento similar. Nesse caso, a pena será de reclusão de quatro a oito anos e multa. Caso o crime seja praticado contra idoso ou pessoa vulnerável, a pena aumenta de um terço ao dobro. E sendo praticado com o uso de servidor de informática mantido fora do país, o aumento da pena pode ser de um terço a dois terços. O Código Penal, em seu art. 155, diz que: "Subtrair, para si ou para outrem, coisa alheia móvel".[24]

Estelionato: No código Penal a pena do estelionato será de reclusão de quatro a oito anos e multa, quando a vítima for enganada e providenciar informações pessoais por meio de alguma rede social. Antigamente o estelionatário, que é o indivíduo causador do engano em alguém e usa isso para causar prejuízo a essa pessoa obtendo uma vantagem ilícita, ele podia ser punido com pena reclusão de um a cinco anos e multa. Conforme há no furto qualificado, a pena para estelionato por meio eletrônico é aumentada se for utilizado servidor fora do território nacional ou se o crime for praticado contra idoso ou vulnerável. Quando o estelionato for praticado por meio de depósito, emissão de cheques sem fundos ou mediante transferência de valores, a competência será definida pelo local do domicílio da vítima. O Código Penal, em seu art. 171, caput, diz que: “Art. 171. Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante

[24] BRASIL. Código Penal Brasileiro. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em 03: mai. 2022.

artifício, ardil, ou qualquer outro meio fraudulento: Pena – reclusão, de 1 (um) a 5 (cinco) anos, e multa.”.[25]

Crimes contra honra: O hackeamento de contas nas redes sociais, a exposição inadequada de pessoas, fraudes em nome de terceiros, tudo isso prejudica a imagem da pessoa que é vítima de uma violação em seu “ciberespaço”, na esfera privada dos meios virtuais. Nota- se que a Internet como a conhecemos hoje ainda é extremamente frágil em termos de proteção e segurança. Para a grande maioria das pessoas a exposição é demais para alguém com a capacidade de hackear querer causar algum dano para chegar a isso com sucesso.

Além de não ter educação formal para lidar com redes internacionais de computadores com medidas mínimas de segurança, esses sistemas ainda estão nos estágios iniciais de desenvolvimento. Há aqueles que buscam usá-la de forma ética, porém existem aqueles que não têm essa barreira moral e estão dispostos a fazê-lo em benefício próprio ou mesmo em detrimento de outros que aprendem a tecnologia ao mesmo tempo.

Venda de Fotos na internet: Algo que vem crescendo absurdamente na internet pelas redes sociais, é a venda de fotos íntimas. Pelas redes sociais, como por exemplo o Facebook e o Instagram, muitos jovens e adolescentes, inclusive menores de idade, oferecem a quem possa interessar imagens de seus corpos, por meio de “packs”, pacotes que contêm fotografias e vídeos sensuais ou com conteúdo proibidos. Existem também pessoas responsáveis por fotografar, comercializar e comprar fotografias infantis nas plataformas digitais, onde se realiza a divulgação e venda dos conteúdos ou “packs”.

Um exemplo de divulgação é Twitter, os cibercriminosos divulgam os conteúdos com os valores e quantidade de fotos ou vídeos que fazem parte do pack. É um esquema muito profundo, que engloba também o WhatsApp e o Telegram, onde o limite de participação de membros em um grupo é de 200 mil participantes. Em grupos como esses dois jovens, um de 18 e o outro de 19 anos que comercializavam conteúdos relacionados a pedofilia foram presos

[25] BRASIL. Código Penal Brasileiro. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em 03: mai. 2022.

neste mês pela polícia, como foi mostrado em reportagem pelo Fantástico[26] na edição do dia 9 de janeiro.

As pessoas que procuram se envolver com essas questões englobando menores de idade estão cometendo crimes. Tanto quem fotografa e comercializa, como quem compra e armazena as imagens, conforme a Lei nº 11.829, de 25/11/2008;

> Art. 1º Os arts. 240 e 241 da Lei no 8.069, de 13 de julho de 1990, passam a vigorar com a seguinte redação:
> "Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente:
> Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.
> § 1º Incorre nas mesmas penas quem agencia, facilita, recruta, coage, ou de qualquer modo intermedeia a participação de criança ou adolescente nas cenas referidas no caput deste artigo, ou ainda quem com esses contracena.
> § 2º Aumenta-se a pena de 1/3 (um terço) se o agente comete o crime:
> I – no exercício de cargo ou função pública ou a pretexto de exercê-la;
> II – prevalecendo-se de relações domésticas, de coabitação ou de hospitalidade; ou
> III – prevalecendo-se de relações de parentesco consangüíneo ou afim até o terceiro grau, ou por adoção, de tutor, curador, preceptor, empregador da vítima ou de quem, a qualquer outro título, tenha autoridade sobre ela, ou com seu consentimento." (NR)
> "Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa." (NR)
> Art. 2º A Lei no 8.069, de 13 de julho de 1990, passa a vigorar acrescida dos seguintes arts. 241-A, 241-B, 241-C, 241-D e 241-E:
> "Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.
> § 1º Nas mesmas penas incorre quem:
> I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;
> II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.
> § 2º As condutas tipificadas nos incisos I e II do § 1o deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo.
> Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
> § 1º A pena é diminuída de 1 (um) a 2/3 (dois terços) se de pequena quantidade o material a que se refere o caput deste artigo.

[26] FANTÁSTICO. **Isso é Fantástico**: Os perigos e crimes da venda de "packs pornográficos" nas redes sociais. [*S. l.*], 9 jan. 2022. Disponível em: https://g1.globo.com/fantastico/podcast/isso-e-fantastico/noticia/2022/01/09/isso-e-fantastico-os-perigos-e-crimes-da-venda-de-packs-pornograficos-nas-redes-sociais.ghtml. Acesso em: 31 out. 2022.

> § 2º Não há crime se a posse ou o armazenamento tem a finalidade de comunicar às autoridades competentes a ocorrência das condutas descritas nos arts. 240, 241, 241-A e 241-C desta Lei, quando a comunicação for feita por:
> I – agente público no exercício de suas funções;
> II – membro de entidade, legalmente constituída, que inclua, entre suas finalidades institucionais, o recebimento, o processamento e o encaminhamento de notícia dos crimes referidos neste parágrafo;
> III – representante legal e funcionários responsáveis de provedor de acesso ou serviço prestado por meio de rede de computadores, até o recebimento do material relativo à notícia feita à autoridade policial, ao Ministério Público ou ao Poder Judiciário.
> § 3º As pessoas referidas no § 2o deste artigo deverão manter sob sigilo o material ilícito referido.
> Art. 241-C. Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual:
> Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.
> Parágrafo único. Incorre nas mesmas penas quem vende, expõe à venda, disponibiliza, distribui, publica ou divulga por qualquer meio, adquire, possui ou armazena o material produzido na forma do caput deste artigo. [27]

2.3 Consequências dos crimes cibernéticos

Além dos exemplos citados acima que nitidamente configuram danos materiais, o crime virtual envolve uma série de consequências danosas para a sociedade.

Uma empresa holandesa de segurança cibernética a Surf Shark[28] em um novo estudo da empresa de segurança cibernética classificou o Brasil como o 4º país que mais sofreu violações de segurança cibernética ao longo do 2º trimestre de 2022, sendo o 1º na América do Sul. A Surf Shark estima que uma em cada cinco pessoas em todo o mundo terá uma violação de dados. Esse é outro ponto muito importante que pode não causar tamanha indignação no curto prazo, mas certamente é prejudicial, são os ataques a bancos de dados para apropriar-se ilegalmente de informações. O sistema legal de proteção[29] de dados pessoais

[27] BRASIL. Lei 11.829/2008. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm#:~:text=LEI%20N%C2%BA%2011.829%2C%20DE%2025%20DE%20NOVEMBRO%20DE,e%20outras%20condutas%20relacionadas%20%C3%A0%20pedofilia%20na%20internet. Acesso em: 03 out. 2022

[28] CONVERGÊNCIA DIGITAL. **Vinte e cinco contas sofrem violações de dados por minutos no Brasil**. [*S. l.*], 18 jul. 2022. Disponível em: https://www.convergenciadigital.com.br/Seguranca/Vinte-e-cinco-contas-sofrem-violacao-de-dados-por-minuto-no-Brasil-60887.html. Acesso em: 30 out. 2022.

precisa enfatizar sobre esse tema no Brasil, é de extrema importância a busca da privacidade e da proteção de dados pessoais e dados em geral na vida das pessoas e das empresas.

[29] CONVERGÊNCIA DIGITAL. **Quase 25 milhões de brasileiros tiveram seus dados violados**. [*S. l.*], 16 dez. 2021. Disponível em: https://www.convergenciadigital.com.br/Seguranca/Quase-25-milhoes-de-brasileiros-tiveram-seus-dados-violados-59064.html?UserActiveTemplate=mobile%2Csite&from%5Finfo%5Findex=506. Acesso em: 30 out. 2022.

3. O MARCO CIVIL E A LEI CAROLINA DIECKMANN 12.737/2012

O marco civil da internet surgiu através da lei 12.965, de 23 de junho de 2014, como citado no capítulo anterior, é responsável por estabelecer instruções de como fazer o uso da internet em todo o território nacional, como as garantias, direitos e deveres de cada pessoa diante da evolução tecnológica. Os primeiros artigos 1°, 3° relata sobre princípios e garantias:

> Art. 1º Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria. (BRASIL, 2014)
> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> I - Garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II - Proteção da privacidade; III - proteção dos dados pessoais, na forma da lei;
> IV - Preservação e garantia da neutralidade de rede;
> V - Preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
> VI - Responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
> VII - preservação da natureza participativa da rede;
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.
> Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte. (BRASIL, 2014)
> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
> IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;
> V - manutenção da qualidade contratada da conexão à internet;
> VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;
> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
> VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
> a) justifiquem sua coleta;
> b) não sejam vedadas pela legislação; e
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

> IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
> X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;
> XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;
> XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e
> XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.
> Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.
> Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no caput, tais como aquelas que:
> I - impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou
> II - em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil. [30]

O autor Teixeira diz:

> Preocupado com a possibilidade de eventualmente haver alguma limitação à liberdade de expressão ou alguma violação da privacidade dos usuários da internet, o Marco Civil expressa que a garantia a esses dois direitos constitucionais é condição para o pleno exercício do direito à acesso à rede mundial de computadores. Ou seja, a violação a esses direitos implica em quebra da própria finalidade do advento do Marco Civil enquanto uma lei federal que objetiva tutelar os usuários da internet.[31]

O Marco Civil da Internet foi criado com o objetivo de envolver a relação ao direito fundamental à privacidade, estabelecer a proteção de dados pessoais de seus usuários e principalmente apontar a necessidade da legislação. Os Projetos de Lei n. 35/2012 foram inicialmente originados pelo Projeto de Lei n. 2.793/2011, que propuseram uma modificação do Projeto de Lei n. 84/99 (Lei Azevedo), foi então publicada pela Lei 12.737/12. Essa lei foi a primeira a ser criada com o objetivo de combater a ocorrência de crimes cibernéticos. A lei foi apelidada com o nome da atriz Carolina Dieckmann, uma figura pública que teve seu computador de uso pessoal inválido e suas fotos íntimas divulgadas. Conforme a presepada

[30] BRASIL. Lei 12.965/2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm . Acesso em: 04 out. 2022.
[31] TEIXEIRA, Tarcísio. **Marco Civil da Internet Comentado**. p. 84. São Paulo: Almedina Brasil, 2016.

que esta situação causou, a lei serviu de um grande instrumento para que ocorresse a punição dos crimes virtuais. Incluindo ao Código Penal os artigos 154-A e 154-B, no qual o legislador autoriza que ocorra a punição daquele infrator que, com a vontade de cometer a conduta delitiva, sem consentimento da vítima, invada qualquer dispositivo informático, com o objetivo de obter, destruir ou alterar informações pessoais ou qualquer coisa pessoal que estejam no dispositivo. Em uma análise, Patrícia Peck Pinheiro, dispõe que:

> Ainda, receberá as mesmas penas da invasão aquele que instala uma vulnerabilidade em um sistema de informação para obter vantagem indevida, por exemplo, um backdoor ou uma configuração para que algumas portas de comunicação à internet fiquem sempre abertas. O usuário de gadgets e dispositivos informáticos comuns estão protegidos contra hackers e pessoas mal intencionadas que abusam de confiança ou buscam intencionalmente devassar dispositivo para se apropriar de dados do computador ou prejudicar o seu proprietário, com a exclusão ou alteração de dados, para que fiquem imprestáveis, ou ainda, informações íntimas e privadas, como fotos, documentos e vídeos. As empresas possuem maior proteção jurídica contra a espionagem digital, pois a obtenção de segredos comerciais e ou informações sigilosas definidas por lei agora também se enquadram na lei.[32]

Entretanto, mesmo existindo uma legislação de suma importância para o combate aos crimes cibernéticos, às crescentes evoluções tecnológicas impedem ainda que a lei esteja totalmente suficiente para suprir todas as necessidades que estes casos trazem. É incontestável que essas ações geram danos irreparáveis às vítimas, e consequências até mesmo irreparáveis, pois atentam contra sua liberdade e à privacidade por se sentirem vulneráveis, com um sentimento de impunidade. É inadmissível que a legislação não obtenha um rigor mais punível nesses crimes, a pena é bem mínima em comparação aos danos recebidos por toda uma exposição pessoal, perda de dados pessoais, dentre tantos outros constrangimentos.

Um dos caso julgados pelo Superior Tribunal de Justiça:

> AGRAVO REGIMENTAL NO AGRAVO EM RECURSO ESPECIAL. CRIME DO ART. 154-A DO CÓDIGO PENAL. INVASÃO DE DISPOSITIVO INFORMÁTICO. REPRESENTAÇÃO. INEQUÍVOCO INTERESSE DE INSTAURAR A AÇÃO PENAL DEMONSTRADO. TESE DE ABSOLVIÇÃO. ÓBICE DA SÚMULA N.º 7 DO SUPERIOR TRIBUNAL DE JUSTIÇA. AGRAVO REGIMENTAL DESPROVIDO. 1. O Superior Tribunal de Justiça sedimentou o entendimento de que a representação da vítima para a investigação ou deflagração da ação penal não exige nenhum rigor formal, bastando a demonstração

[32] PINHEIRO, Patrícia Peck. **Direito Digital.** 4. Ed. São Paulo: Saraiva, 2010.

> inequívoca do interesse da vítima ou do representante legal em iniciar a persecução criminal. 2. Na hipótese, como bem retratado no acórdão recorrido, além de mencionar as supostas ameaças que estaria sofrendo, a Vítima também noticiou que o Acusado "publicou fotos íntimas em redes sociais sem sua permissão para denegrir sua imagem, fotos essas que estavam em seu celular que o Acusado furtou", o que 9 demonstra o inequívoco interesse de representação também quanto ao delito do art. 154-A do Código Penal. 3. No caso, o pleito recursal de absolvição implicaria, necessariamente, o reexame de todo o conjunto fático-probatório, o que não se coaduna com a via eleita, em face do óbice do enunciado n.º 7 da Súmula do Superior Tribunal de Justiça. 4. Agravo regimental desprovido. 05/02/2019 (STJ - AgRg no AREsp: 1394738 ES 2018/0296072-6, Relator: Ministra LAURITA VAZ, Data de Julgamento: 05/02/2019, T6 - SEXTA TURMA, Data de Publicação: DJe 22/02/2019 RMDPPP vol. 88 p. 109). É claro no texto legal que a conduta do réu é elemento de dolo, não podendo mencionar a responsabilização pela figura culposa, portanto, é através do dolo que se concretiza a prática do delito, pois o agente tem a intenção de praticar a conduta. Além do mais, após o acontecimento do fato, a vítima deve promover a sua representação, ou seja, será por intermédio de ação penal pública condicionada. Por conseguinte, dar-se-á sequência no procedimento para se apurar a conduta. É de extrema necessidade a representação da vítima, para que seja instaurada a investigação criminal e a ação penal. Com ações como estas será possível inibir práticas como essas, de forma que possibilite reduzir a ineficiência da lei protetora. [33]

3.1 A ineficácia que encontramos na lei da Carolina Dieckmann

A Lei Carolina Dieckmann (Lei 12.737/12), que dispõe sobre a tipificação criminal dos delitos no âmbito virtual, no dia 03 de dezembro de 2022, completará 10 anos de sanção. Embora isso, pode-se dizer que a efetividade foi baixa neste período. Pois constatam-se diversas vulnerabilidades na aplicabilidade das normas da Lei 12.737, uma delas é a dificuldade de produção de prova, que é importante para que haja punição sobre a adulteração, modificação ou qualquer ato prejudicial de invadir dispositivo informático com a intenção de prejudicar. Para maiores esclarecimentos, é necessário compreender que essa interpretação pode variar entre a consumação e tentativa, sendo estas como fatores qualificativos da pena. Ademais, com o advento desta lei é possível encontrar determinados grupos sociais que são mais vulneráveis a utilização indevida do dispositivo eletrônico, como por exemplo, crianças e adolescentes.

[33] BRASIL. SUPERIOR TRIBUNAL DE JUSTIÇA. **Crime cibernético tomou lugar de roubos e furtos na pandemia, diz ministro Humberto Martins.** 2020. Disponível em: http://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/Crime-cibernetico-tomou-lugar-de-roubos-e-furtos-na-pandemia--diz-ominstro-Humberto-Martins.aspx. Acesso em: 23 nov. 2022

O grupo de crianças e adolescentes, em regra, já é um grupo de vulnerabilidade, principalmente quando trata-se de crimes cibernéticos. Essa população possui maiores fragilidades por conta da construção da personalidade, quando esses crimes ocorrem passam a ter maior relevância até mesmo na construção social e de personalidade daquele agente, ao qual podem gerar maiores consequências. Por conta disso, há aplicações especiais desta lei, ao qual passa a ser possível o aumento de pena e modalidade equiparada e qualificada, suspensão condicional do processo e outros.

Outro fator que influencia na aplicabilidade da Lei 12.737 é a ausência de rastros por utilização de plataformas ocultas, como é o exemplo da Deep Web. Essas plataformas são utilizadas apenas por pessoas que possuem um alto índice de conhecimento no mundo eletrônico, ao qual é quase impossível uma pessoa leiga conseguir acesso. Sem dúvidas, a dificuldade de acessar esses meios implica diretamente na obtenção de meios comprobatórios por conta de que na maioria das vezes não deixam rastros.

Ademais, a constante evolução dos meios digitais, como implementação de uso em operações de transações bancárias, dificultou que o ordenamento jurídico acompanhasse de forma segura todas essas mudanças. Com esse obstáculo, impossibilitou ainda que fossem implementadas maiores formas de segurança.

3.2 Das provas

Incontestavelmente as provas que são encontradas no ambiente virtual são muito frágeis, e podem ser danificadas ou até mesmo perecer uma prova coletada. O esforço obtido no trabalho de recolhimento da prova deve ser realizado com bastante profissionalismo, pois existe uma dificuldade de localização dos autores. As investigações iniciaram-se com a Notitia Criminis (notícia do crime) que vai ser informado ao Delegado de Polícia, Juiz ou Ministério Público sobre o ato delituoso, isso vai ocasionar uma fase técnica para apurar as informações que chegaram à autoridade, relatos expostos pela própria vítima e assim iniciar as buscas pelo objeto e material que demonstre a prática delituosa, sejam em computadores, telefones, tablets entre outros. Além disso, será feito um Boletim de Ocorrência que será o caminho para dar início à instauração do Inquérito Policial e na fase de investigação coletará

provas, mas para determinados casos é indispensável que haja uma autorização judiciária, por exemplo, em casos da quebra de dados, acessos, que serão essenciais para a investigação. Quando for localizado o objeto que ensejou o ato serão feitas buscas no local pela polícia através de uma autorização judicial, por exemplo, um mandado de busca e apreensão do objeto que será emitido pelos juízes competentes, possibilitando a realização dos demais atos investigatórios. Porém, toda essa parte investigativa irá depender da autorização do juiz.

Os tipos de crimes cibernéticos tem como evidência: telefone, máquina fotográfica, computadores, pen drives, registros de equipamentos de rede, como o e-mail. Além das evidências, há provas que podem ser obtidas através da busca no histórico de navegadores, arquivos digitais, fotos, vídeos, registros de conversas, registros em servidores. Entretanto, as provas digitais podem se Comprometem e, em última análise, atrapalham a investigação e até mesmo a identificação do perpetrador. Com a tecnologia contemporânea, o risco de tais crimes está aumentando. Além dos sistemas de computação em nuvem e outros meios utilizados por esses autores, a cada dia são lançados mais e mais modernos dispositivos com enormes capacidades de armazenamento. No campo penal, assim como em outros ramos do direito, para atribuir responsabilidade penal aos indivíduos e, assim, impor as sanções penais adequadas, é necessário determinar os crimes cometidos pelo suposto infrator. Para que um juiz aplique sanções penais, deve haver provas de que o réu foi o autor. O significado da palavra prova no meio jurídico é: “Instrumento por meio do qual é formado o convencimento/convicção do juiz a respeito da veracidade ou falsidade do que é alegado, assim como da ocorrência ou Prova - Novo CPC - (Lei nº 13.105/15) - Dicionário jurídico – DireitoNet. 15 não dos fatos controvertidos no processo. (DireitoNet, Prova- Novo CPC- (Lei n° 13.105/15), 2022.”

Como citado acima, a prova é um dos grandes caminhos no âmbito jurídico que busca garantir a efetiva repreensão do criminoso. Mas no âmbito virtual, o autor do crime e a própria vítima enfrentam grandes dificuldades em provar o crime e atribuir o crime ao verdadeiro culpado. Vale ressaltar que, embora os meios tecnológicos possam ajudar a desvendar certos crimes, também existem limitações que dificultam a localização dos criminosos. Na era digital, as pessoas se escondem atrás de telas de computador em sites obscuros. Alcançar os criminosos que exploram essas situações tornou-se uma verdadeira operação "007". Na maioria das vezes, os criminosos não deixam vestígios de suas ações,

escondendo-se na sombra do anonimato. É importante ressaltar que a prova do fato não basta, tem que ser verificada e tem que ser legítima para surtir efeito efetivo. A Constituição e o Código de Processo Penal não permitem a produção de provas em meios jurídicos e online sem prévia autorização judicial.

> Para o doutrinador Fernando da Costa Tourinho Filho, as provas são:
> Que se entende por prova: Provar é, antes de mais nada, estabelecer a existência da verdade; e as provas são os meios pelos quais se procura estabelecê-la. É demonstrar a veracidade do que se afirma, do que se alega. Entendem-se, também, por prova, de ordinário, os elementos produzidos pelas partes ou pelo próprio Juiz visando a estabelecer, dentro do processo, a existência de certos fatos. É os instrumentos de verificação do thema probandum.[34]

A identificação pericial dos vestígios encontrados na prática de crimes cibernéticos é fundamental para que os processos criminais sejam elaborados por meio de laudos periciais e os juízes possam chegar a uma decisão com o auxílio de provas técnicas. Para o bom andamento do processo penal, é necessário vincular a significação do fato ao autor, sendo, portanto, imprescindível a comprovação de sua significação. Para alcançar essa conexão factual, a forma probatória do sistema jurídico fornece uma estrutura genuína de ferramentas que podem auxiliar na busca da verdade. A prova, seja ela perícia, documentação ou comprovação, é, portanto, uma aliada essencial na comprovação da importância. Não será diferente no contexto do ciberespaço, onde mesmo com os meios eletrônicos já disponíveis, a justiça ainda luta para provar a autoria de um crime rastreando seus 16 usuários.

Porém, os meios de comprovação são parecidos com os oferecidos aos crimes ocorridos no meio físico. Para comprovar esses crimes existem diversas formas usuais e ilícitas no âmbito jurídico, por exemplo: depoimentos, interrogatório do acusado, acareação, busca e apreensão entre outros, possuindo especial valor, a depender da espécie, o conteúdo arquivado no dispositivo da vítima e no dispositivo utilizado pelo ofensor, bem como a prova pericial.

[34] TOURINHO FILHO, Fernando da Costa. **Manual de processo penal**. São Paulo: Saraiva, 2012. P. 563.

3.3 A lei Carolina Dieckmann nas delegacias especializadas

A lei 12.735/12 conhecida como Lei Azeredo, vem conceituar para os órgãos da polícia judiciária o que é necessário para a criação de setores específicos para o combate aos crimes virtuais. Apesar da lei promulgada prever a criação dos setores especializados em crimes virtuais, ainda é raro encontrá-los dentro do sistema judiciário brasileiro. As delegacias especializadas ainda são poucas diante da demanda criminal existente. O principal objetivo dessas delegacias é analisar a ocorrência de crimes de acordo com sua profissão, portanto, esse tipo de delegacia não funcionava antes dessa legislação. Assim, como qualquer procedimento investigativo, quando ocorrer um crime dessa natureza, as autoridades policiais cumprirão abstratamente a pena máxima, instaurada seja por T.C.O (termo circunstanciado de ocorrência) ou por inquérito policial. A responsabilidade pela investigação destes e de muitos outros crimes cabe à Polícia Judiciária. Embora a polícia civil esteja sobrecarregada com o número de incidentes registrados a cada dia, as autoridades e seus agentes não estão preparados para fazê-lo rapidamente devido à falta de pessoal qualificado e investimento material. Isso reforça ainda mais a necessidade de ampliar as delegacias especializadas com as estruturas humanas e materiais necessárias para que a apuração e a punição dos crimes virtuais sejam mais efetivas.

A obtenção de bons resultados nessas investigações é fundamental, e as informações armazenadas nos dispositivos tecnológicos dos criminosos ou mesmo das vítimas devem ser coletadas o mais rápido possível antes que sejam perdidas. Quase sempre, o acesso à informação é retardado, perdido ou alterado devido à demora da polícia e à falta de preparo para contornar as investigações e proteger os criminosos. Portanto, é imperativo ser ágil na execução dessas ordens e na coleta de dados. Portanto, mesmo com todos os mecanismos possíveis para rastrear os autores dos crimes, sempre será difícil interligar os criminosos com os dispositivos utilizados. Com sistemas mais eficientes e coleta imediata de dados, as conclusões serão mais efetivas e poderão ser obtidas provas suficientes para responsabilizar os criminosos. Estas medidas são necessárias porque a maioria dos criminosos e a maioria da população ainda acreditam que a internet é uma “terra sem lei” isso é uma consequência da falta de punibilidade dos criminosos que utilizam este meio para a prática de uma diversidade

de crimes. Conforme uma pesquisa realizada no SefaNet.com verifica-se que em 2021 houve um crescente número de denúncias no site, conforme abaixo demonstra:

> Indicadores da Central Nacional de Denúncias de Crimes Cibernético: Em 2021, a Central de Denúncias recebeu e processou 150.095 denúncias anônimas envolvendo 71.095 páginas (URLs) distintas (das quais 32.538 foram removidas) escritas em 10 idiomas e hospedadas em 8.926 domínios diferentes, de 170 diferentes TLDs e conectados à Internet através de 9.900 números IPs distintos, atribuídos para 68 países em 6 continentes. As denúncias foram registradas pela população através dos 3 hotlines brasileiros que integram a Central Nacional de Denúncias de Crimes Cibernéticos.[35]

3.4 Da adversidade de punição e sanção aplicada

O Brasil tem tentado modificar o sistema penal brasileiro para obter melhorias quando o assunto é os crimes cibernéticos. Sabe-se que infelizmente não é uma tarefa fácil no âmbito virtual. Na maioria das vezes não se sabe quem está por trás do crime, se realmente ele é realizado por uma pessoa ou um software programado para executar o ato criminoso. O Brasil tem cerca de 155,7 milhões[36] de usuários de internet, segundo pesquisa realizada em 2022, e esse número vem crescendo absurdamente.

Com o aumento da população a imensidão das inovações tecnológicas, acaba sendo um desafio para a localização dos criminosos existentes, visto que é necessário para a punição destes. O Sistema legislativo brasileiro é especialista em criar leis, sejam de qualquer caso que der um pouco mais de repercussão, é criado uma lei para punir o ato. Entretanto, não adianta criar leis e mais leis se não funcionam ou se deixam grandes lacunas interpretativas. Um levantamento de dados, feito pela Febraban (Federação Brasileira de Bancos) apontou dados assustadores durante esta pandemia social de isolamento, houve aumento de 80% nas tentativas de ataques de phishing no Brasil. Devido a isso surge uma insegurança de que o que é feito nos âmbitos virtuais não tem punição. Ou caso tenha, o questionamento se vale a pena correr o risco, já que a punição é tão branda. As penas para quem comete crimes virtuais é de detenção de 3 (três) meses a 1 (um) ano, e multa ou de reclusão, de 6 (seis) meses a 2

[35] SEFANET **Indicadores da Central Nacional de Denúncias de Crimes Cibernético**. [*S. l.*], 9 dez. 2022. Disponível em: https://indicadores.safernet.org.br/index.html. Acesso em: 30 out. 2022.
[36] GOV. **Aumenta para 90% o número de domicílios com internet no Brasil**. [*S. l.*], 16 set. 2022. Disponível em: https://www.gov.br/mcom/pt-br/noticias/2022/setembro/aumenta-o-numero-de-domicilios-com-internet-no-brasil. Acesso em: 9 dez. 2022.

(dois) anos, e multa, se a conduta não constitui crime mais grave. Neste caso poderá ter agravantes, mas são tão raros os casos que são classificados como graves:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico. § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas. §
> 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III-Presidente da Câmara dos Deputados, do Senado Federal, da Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal;
> ou IV - Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (BRASIL, 1940) .
>
> Inserção de dados falsos em sistema de informações (Incluído pela Lei nº 9.983, de 2000)
> Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: (Incluído pela Lei nº 9.983, de 2000))
> Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa. (Incluído pela Lei nº 9.983, de 2000)
> Modificação ou alteração não autorizada de sistema de informações (Incluído pela Lei nº 9.983, de 2000)
> Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente: (Incluído pela Lei nº 9.983, de 2000)
> Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa. (Incluído pela Lei nº 9.983, de 2000)
> Parágrafo único. As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado. (Incluído pela Lei nº 9.983, de 2000)

Grande parte da população não acredita que os infratores de crimes cibernéticos serão punidos ou sequer levados à justiça. Isso demonstra o quanto a falta de punição e efetivação da legislação penal brasileira precisa de melhorias e o quanto é necessário ser trabalhado para efetivar a punição dos crimes cibernéticos. Principalmente as investigações, que necessitam serem mais eficientes e o ordenamento jurídico precisa aplicar a sanção, mas para que isso ocorra é preciso ter a total certeza da prática do crime, fazendo a comprovação da autoria, materialidade ou a existência de indícios de que o sujeito praticou o crime. Porém, nos caso não há a comprovação, o juiz poderá absolver o réu, respaldado no artigo 386, VII, do Código de Processo Penal.

> Art. 386. O juiz absolverá o réu, mencionando a causa na parte dispositiva, desde que reconheça:
> (...)
> VII - não existir prova suficiente para a condenação.[37]

Portanto, para se imputar um crime a alguém é preciso que haja a comprovação de sua materialidade, pois, somente a contestação da ocorrência de um crime não é elemento suficiente para uma condenação criminal. Os fatos devem estar relacionados ao réu e os seus atos devem ser típicos, antijurídicos e culpáve**is.**

3.5 Ampliação da incidência da lei Carolina Dieckmann na pandemia COVID-19

Existem várias maneiras delitivas da configuração dos crimes virtuais, como citado anteriormente um indivíduo pode sofrer danos pela prática de algum tipo de crime cibernético. Conforme o estudo da multinacional Symantec, publicado pelo site correiobraziliense.com.br, no Brasil, a cada 60 segundos cerca de 54 pessoas são 12 Falta de lei sobre crimes virtuais leva à impunidade, diz especialista 20 vítimas de algum crime cibernético. O meio virtual vem se tornando cada vez mais um campo fértil para os cibercriminosos. Nos anos de 2020/2021, o número de ocorrência dos chamados crimes cibernéticos aumentaram muito, em decorrência da pandemia do COVID-19, alastrada por todo mundo. Devido ao isolamento social e a limitação do direito de ir e vir, trouxe como

[37] BRASIL. Código Penal Brasileiro. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em 03: mai. 2022.

consequência que as pessoas utilizassem mais as ferramentas sociais, principalmente para realizar trabalhos em home office, que se tornou cada vez mais corriqueiro diante da situação pandêmica vivenciada.

O advogado e perito José Antônio Milagre, especializado em Direito Digital e Crimes Cibernético diz:

> Tivemos um aumento de crimes cibernéticos contra o patrimônio a partir do momento em que profissionais tiveram que trabalhar em home office, sem que a empresa tivesse um programa de segurança em teletrabalho. Resultado, muitos golpes, fraudes e códigos maliciosos que infectam não só o computador do empregado, mas a rede da empresa. O aumento das reuniões e atividades on-line, diante do distanciamento, também fomentou novas abordagens. Recebemos notificações de golpes do leilão, invasão de reuniões sigilosas e até transferências indevidas de valores a partir da invasão a contas bancárias... (Diário do Litoral, O Brasil sofreu mais de 3,4 bilhões de tentativas de ataques cibernéticos em 2020, 2021) É evidente que usuários logados na rede de internet não estão preparados para as armadilhas cibernéticas espalhadas no mundo virtual, que criam teias poderosas e que, na maioria das vezes, é quase impossível perceber seu caráter malicioso. O problema é que quanto mais se usa estas ferramentas, mas as pessoas estão expostas aos crimes cibernéticos.

Conforme os crimes cibernéticos foram crescendo, o Brasil buscou aderir à Convenção Budapeste, com o objetivo de facilitar no andamento dos casos e assim ter um acesso mais rápido a as provas que os cibercriminosos deixavam pelo "caminho", conforme o trecho abaixo da Agência Brasil:

> O Brasil depositou, junto ao Conselho da Europa, sediado em Estrasburgo, França, a carta de adesão à Convenção sobre o Crime Cibernético, também conhecida como Convenção de Budapeste. Com isso, conclui-se o processo de acessão do país ao acordo, que tem por objetivo facilitar a cooperação internacional no combate aos crimes cibernéticos. A informação foi divulgada nesta quarta-feira (30), em nota conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública.
> A Convenção de Budapeste reúne grande número de países com os quais o Brasil compartilha a maior parte dos casos de cooperação jurídica internacional hoje em tramitação e serve de base de colaboração contra ampla variedade de crimes realizados por via cibernética. Somando-se a 67 membros, o país contará com ferramenta adicional para combater o crime cibernético, que exige meios de cooperação internacional céleres, mediante os quais os órgãos responsáveis possam requerer e compartilhar as provas necessárias.
> As autoridades brasileiras terão, assim, acesso mais ágil a provas eletrônicas produzidas sob jurisdição estrangeira, o que repercutirá positivamente em termos de condenação penal dos crimes cibernéticos.[38]

[38] GOV. **Aprovada adesão do Brasil à Convenção de Budapeste sobre o Crime Cibernético**: Iniciativa faz parte de demanda oficial do Ministério da Justiça e Segurança Pública. [S. l.], 21 dez. 2021. Disponível em:

3.6 Denúncias de Crimes na Internet

Desde a promulgação da Lei 12.737/2012, o Brasil conta com várias delegacias especializadas no tratamento de crimes cibernéticos. Porém o número ainda é considerado pequeno mediante ao crescente número, além de que as investigações tendem a se concentrar apenas em crimes envolvendo problemas financeiros. No entanto, as provas podem ser coletadas e relatadas a qualquer delegacia, portanto, também é viável a propositura de ações judiciais por meio do setor público, que conta com procuradores especializados nos estados. Crimes cibernéticos como fraudes, roubos e desfalques usando dispositivos eletrônicos como celulares, computadores e tablets estarão sujeitos a penalidades mais severas. Conforme a Lei nº 14.155 de 2021, que foi publicada no Diário Oficial da União pelo presidente Jair Bolsonaro, decreta:

> O PRESIDENTE DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:
> Art. 1º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar com as seguintes alterações:
> "Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.

Essa lei é derivada do Projeto de Lei[39] (PL) 4.554/2020 do senador Izalci Lucas (PSDB-DF). Foi aprovado pelo Senado, este texto altera o Código Penal (Lei nº 2.848 de 1940) para que haja aumento das penas como invasão de aparelho, furto qualificado e desfalque, que ocorrem em meios digitais conectados ou não à Internet. Com a nova redação do código, realizar a invasão de equipamentos de informática acarreta pena de um a quatro anos de prisão e multa, entretanto, aumenta de um terço para dois terços se a invasão causar danos financeiros. Anteriormente, as penas aplicáveis eram de três meses a um ano de detenção e multa. As penalidades se aplicam a qualquer pessoa que hackear um dispositivo para obter, adulterar ou destruir dados ou informações sem a autorização do proprietário, ou instalar uma vulnerabilidade para obter uma vantagem ilegal. Se a invasão resultar na

https://www.gov.br/mj/pt-br/assuntos/noticias/aprovada-adesao-do-brasil-a-convencao-de-budapeste-sobre-o-crime-cibernetico. Acesso em: 8 nov. 2022.

[39] Portal da Câmara dos Deputados (camara.leg.br)

aquisição de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações confidenciais ou controle remoto não autorizado do dispositivo comprometido.

CONCLUSÃO

É inegável que a internet traz benefícios para toda à humanidade, facilitando a vida das pessoas com milhares de benefícios que somente a tecnologia pode nos proporcionar. Entretanto, podemos concluir que infelizmente ainda surge e continua crescente os índices de crimes virtuais no nosso dia a dia, mesmo diante da evolução da legislação, segue sendo muito comum a ocorrência dos crimes.

Durante as evoluções constantes que vem ocorrendo, pode-se observar que anteriormente a legislação ainda era muito “leve” em relação a punição de atos criminosos no mundo virtual, e por vários anos a penalidade chegava a ser considerada “ilustrativa”. Porém, devido à Convenção de Budapeste no Brasil, podemos acreditar em uma severidade bem ampla em relação a aplicabilidade das leis que regem o direito digital, tornando se assim um marco de valor enorme para a nossa legislação e para a nossa sociedade. Com a entrada do Brasil na Convenção de Budapeste, é criada em nós uma expectativa de que isso tenha um impacto positivo, de uma punibilidade bem maior, quando ocorrer futuramente algo relacionado com um crime virtual.

Diante de tudo que foi exposto, foi definido neste trabalho monográfico as várias formas tecnológicas dos ataques que são realizados no âmbito virtual para se referir aos crimes cibernéticos, além de definições próprias de cada doutrinador que está definindo esses delitos. As outras formas peculiares sobre esses crimes, como o ciberespaço, malwares e hackers, dentre outros.

Pode-se dizer que o Direito Penal, conclui que a tecnologia da informação faz parte de um bem jurídico-penal, sendo suscetível às consequências que isso traz e revelando-se numa dinâmica existente há algum tempo, principalmente aquele que vem se desenvolvendo nos últimos tempos: A dos crimes cibernéticos. Conforme tudo que vem acontecendo no tratamento dos crimes cibernéticos, realizou-se buscas para conceituar esses crimes cibernéticos, no qual conclui - se que se torna um fato típico, ilícito e culpável cometido contra uma pessoa ou por meio da tecnologia da informação. Crimes esses abordados nos próprios ordenamento jurídico brasileiro, que estão previstos nos seguintes dispositivos: art.

154-A do Código Penal; 266 do Código Penal; art. 10 da Lei 9.296/96; e arts. 313-A e 313-B do Código Penal.

Considerando que posteriormente, esse presente trabalho buscou abordar algumas das questões comumente discutidas na pesquisa do cibercrime: técnicas e comportamento criminoso, cenas de crime e autoria. Em relação às primeiras, observa-se que não é lucrativo tipificar as tecnologias cibernéticas, pois elas seguem em uma constante mudança e aprimoramento; na verdade, o comportamento deve ser tipificado incluindo-se porém não se limitando a tecnologias. Em relação ao local do crime, verifica-se que como nosso código penal emprega a teoria da ubiquidade, esse problema tecnicamente não é um grande problema, visto que será considerado como o local do crime ou o local do crime que deve produzir seus resultados. Concluiu que a legislação criminal do Brasil sobre crimes cibernéticos normalmente não é falha, mas observou que melhorias são extremamente necessárias para proteger melhor os ativos legais e criminais no aspecto da tecnologia da informação.

Uma questão mais complexa diz respeito aos autores de crimes cibernéticos, mas informações baseadas no Ministério da Justiça e na Lei 12.965/14 demonstram os caminhos que as forças de investigação devem seguir para encontrar os autores de atos cibercriminosos. A obtenção de endereços IP por meio de conhecimento profissional; Obtenção de informações sobre direitos de propriedade intelectual de fornecedores com autorização judicial; Finalmente, sob autorização de autoridades judiciais, prosseguir com as diligências relativas à violação de sigilo telefônico No último tópico, a questão é analisar possíveis deficiências na legislação penal brasileira sobre crimes cibernéticos, tomando como parâmetros a Convenção sobre Crimes Cibernéticos (Convenção de Budapeste) e a Comissão Parlamentar de Inquérito sobre Crimes Cibernéticos, no âmbito da Câmara dos Deputados. Além disso, no que diz respeito à identificação da autoria, embora seja fácil rastrear o computador em que ocorreu o crime,

Quando se utiliza a biometria juntamente com a prisão em flagrante, o computador ativo são boas opções na busca de soluções propostas a fim de resolver tal problema. Portanto, considerando a grande capacidade de volatilidade dos meios que servirão como prova do

crime cibernético praticado, o instituto da produção antecipada de provas ganha importância, diante da possibilidade de perecimento das provas.

Por fim, devido ao crime ocorrido por uma invasão ao seu computador, a vida da atriz Carolina Dieckmann mudou radicalmente, houve então a proposta da lei apresentada em novembro de 2011, que foi aprovada um ano após sua apresentação. Sabendo de todo o transtorno que passou, a atriz acolheu a causa e cedeu o seu nome que é conhecido como à lei da Carolina Dieckmann.

BIBLIOGRAFIA

ABRAMOVAY, Pedro. **O Marco Civil e a Política dos Netos**. [*S. l.*], 7 maio 2014. Disponível em: https://sul21.com.br/opiniao/2014/05/o-marco-civil-e-a-politica-dos-netos-por-pedro-abramovay/. Acesso em: 2 out. 2022.

ACCENTURE**. The state of cybersecurity resilience 2021.** [*S. l.*], 3 nov. 2021. Disponível em: https://www.accenture.com/pt-pt/insights/security/invest-cyber-resilience. Acesso em: 25 out. 2022.

AGÊNCIA BRASIL. *In*: CAMARGO, Marcelo. **Ipea**: 11% dos trabalhadores fizeram home office ao longo de 2020. Rio de Janeiro, 15 jul. 2021. Disponível em: https://agenciabrasil.ebc.com.br/economia/noticia/2021-07/ipea-11-dos-trabalhadores-fizeram-home-office-ao-longo-de-2020. Acesso em: 2 out. 2022.

AMARIZ, Luiz Carlos. Infoescola. **Hackers e Crackers**. [*S. l.*]. Disponível em: https://www.infoescola.com/informatica/hackers-e-crackers/. Acesso em: 25 out. 2022.

ARAYA , Elizabeth Roxana Mass; VIDOTTI , Silvana Aparecida Borsetti Gregório. **Criação, proteção e uso legal de informação em ambientes da World Wide Web**. São Paulo: Editora Unesp, 2010. 146 p. Disponível em: https://static.scielo.org/scielobooks/fdx3q/pdf/araya-9788579831157.pdf. Acesso em: 2 out. 2022.

ARRAES, Bruno; CARVALHO, Marcela Melo de. Suicídio e pornografia de vingança. Disponível em: Acesso em: 01 out. 2022.
BRASIL. Constituição Federal da República Federativa do Brasil de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm . Acesso em: 20 out. 2022.

BRASIL. Código Penal Brasileiro. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em 03: mai. 2022.

BRASIL. Lei 11.340/2006. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11340.htm. Acesso em: 03 out. 2022.

BRASIL. Lei 11.829/2008. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm#:~:text=LEI%20N%C2%BA%2011.829%2C%20DE%2025%20DE%20NOVEMBRO%20DE,e%20outras%20condutas%20relacionadas%20%C3%A0%20pedofilia%20na%20internet. Acesso em: 03 out. 2022

BRASIL. Lei 12.737/2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm . Acesso em: 03 out. 2022.

BRASIL. Lei 12.965/2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm . Acesso em: 04 out. 2022.
BRASIL. Lei nº 13.718/2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13718.htm . Acesso em: 20 out. 2022.

BRASIL. SUPERIOR TRIBUNAL DE JUSTIÇA. **Crime cibernético tomou lugar de roubos e furtos na pandemia, diz ministro Humberto Martins.** 2020. Disponível em: http://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/Crime-cibernetico-tomou-lugar-de-roubos-e-furtos-na-pandemia--diz-ominstro-Humberto-Martins.aspx. Acesso em: 23 nov. 2022

CAETANO, Érica. **O que é hacker?**; Brasil Escola. Disponível em: https://brasilescola.uol.com.br/informatica/o-que-e-hacker.htm. Acesso em: 31 de out. de 2022.

CAMPOS, Lorraine Vilela. O que são Fake News?; Brasil Escola. Disponível em: https://brasilescola.uol.com.br/curiosidades/o-que-sao-fake-news.htm. Acesso em 08 de dez. de 2022.

CONVERGÊNCIA DIGITAL. **Vinte e cinco contas sofrem violações de dados por minutos no Brasil**. [*S. l.*], 18 jul. 2022. Disponível em: https://www.convergenciadigital.com.br/Seguranca/Vinte-e-cinco-contas-sofrem-violacao-de-dados-por-minuto-no-Brasil-60887.html. Acesso em: 30 out. 2022.

CONVERGÊNCIA DIGITAL. **Quase 25 milhões de brasileiros tiveram seus dados violados**. [*S. l.*], 16 dez. 2021. Disponível em: https://www.convergenciadigital.com.br/Seguranca/Quase-25-milhoes-de-brasileiros-tiveram-seus-dados-violados-59064.html?UserActiveTemplate=mobile%2Csite&from%5Finfo%5Findex=506. Acesso em: 30 out. 2022.

FACHINI, Tiago. **Quais os crimes virtuais e golpes digitais mais comuns?**. [*S. l.*], 9 dez. 2014. Disponível em: https://tiagofachini.jusbrasil.com.br/artigos/156312969/quais-os-crimes-virtuais-e-golpes-digitais-mais-comuns. Acesso em: 31 out. 2022.

FANTÁSTICO. **Isso é Fantástico**: Os perigos e crimes da venda de "packs pornográficos" nas redes sociais. [*S. l.*], 9 jan. 2022. Disponível em: https://g1.globo.com/fantastico/podcast/isso-e-fantastico/noticia/2022/01/09/isso-e-fantastico-os-perigos-e-crimes-da-venda-de-packs-pornograficos-nas-redes-sociais.ghtml. Acesso em: 31 out. 2022.

FINTECHS. **Relatório**: O estudo de fraude de identidade de 2021. [*S. l.*], 7 abr. 2021. Disponível em: https://fintechs.com.br/relatorio-o-estudo-de-fraude-de-identidade-de-2021/. Acesso em: 25 out. 2022.

FORBES. *In*: HIGH, Peter. **A Conversation With The President Of The World's First Non-Profit, Tuition-Free, Accredited, Online University**. [*S. l.*], 3 mar. 2014. Disponível em: https://www.forbes.com/sites/peterhigh/2014/03/03/a-conversation-with-the-president-of-worlds-first-non-pro%EF%AC%81t-tuition-free-accredited-online-university/?sh=305ecdf45c7d. Acesso em: 2 out. 2022.

GOV. **Aumenta para 90% o número de domicílios com internet no Brasil**. [*S. l.*], 16 set. 2022. Disponível em: https://www.gov.br/mcom/pt-br/noticias/2022/setembro/aumenta-o-numero-de-domicilios-com-internet-no-brasil. Acesso em: 9 dez. 2022.

GOV. **Aprovada adesão do Brasil à Convenção de Budapeste sobre o Crime Cibernético**: Iniciativa faz parte de demanda oficial do Ministério da Justiça e Segurança Pública. [S. l.], 21 dez. 2021. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/aprovada-adesao-do-brasil-a-convencao-de-budapeste-sobre-o-crime-cibernetico. Acesso em: 8 nov. 2022.

KASPERSKY. **O que são crimes cibernéticos?**: Como se proteger dos crimes cibernéticos?. [*S. l.*]. Disponível em: https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime. Acesso em: 25 out. 2022.

LEWIN, Tamar. **Israeli Entrepreneur Plans a Free Global University That Will Be Online Only**. [*S. l.*], 25 jan. 2009. Disponível em: https://www.nytimes.com/2009/01/26/education/26university.html#:~:text=An%20Israeli%20entrepreneur%20with%20decades,the%20University%20of%20the%20People. Acesso em: 2 out. 2022.

OLIVEIRA, Marco Antonio Rodrigues de. **Crime nas redes**: fotos de menores de idade são vendidas na internet. [*S. l.*], 31 jan. 2022. Disponível em: https://megaminas.com.br/colunistas/seguranca-e-cidadania/crime-nas-redes-fotos-de-menores-de-idade-sao-vendidas-na-internet. Acesso em: 31 out. 2022.

PETRIN, Natália. Redes Sociais. **Todo Estudo**. Disponível em: https://www.todoestudo.com.br/historia/redes-sociais. Acesso em: 08 de dec. 2022.

PINHEIRO, Patrícia Peck. **Direito Digital**. 4. Ed. São Paulo: Saraiva, 2010.

PSICANALISE CLÍNICA. **Conhecendo os Benefícios e Malefícios da Internet.** [*S. l.*], 3 jan. 2020. Disponível em: https://www.psicanaliseclinica.com/beneficios-e-maleficios-da-internet/. Acesso em: 2 out. 2022.

RIBEIRO, Paulo. **Benefícios e Malefícios da Internet**. [*S. l.*]. Disponível em: http://efaa1.weebly.com/internet---benefiacutecios-e-maleficios.html. Acesso em: 2 out. 2022.
ROSSINI, Augusto Eduardo de Souza. Informática, telemática e direito penal. São Paulo: Memória Jurídica, 2004.

SEFANET. **Indicadores da Central Nacional de Denúncias de Crimes Cibernético**. [*S. l.*], 9 dez. 2022. Disponível em: https://indicadores.safernet.org.br/index.html. Acesso em: 30 out. 2022.

TEIXEIRA, Tarcísio. **Marco Civil da Internet Comentado**. São Paulo: Almedina Brasil, 2016.

TOURINHO FILHO, Fernando da Costa. **Manual de processo penal**. São Paulo: Saraiva, 2012. P. 563.

VOLPATO, Bruno. **Ranking**: as redes sociais mais usadas no Brasil e no mundo em 2022, com insights e materiais. [*S. l.*], 23 maio 2022. Disponível em: https://resultadosdigitais.com.br/marketing/redes-sociais-mais-usadas-no-brasil/. Acesso em: 2 out. 2022.