UNIVERSIDADE TIRADENTES – UNIT
CURSO DE GRADUAÇÃO EM DIREITO

LEANDRO LIMA NEVES

CIBERCRIMES E O ORDENAMENTO JURÍDICO BRASILEIRO

Aracaju
2020

LEANDRO LIMA NEVES

CIBERCRIMES E O ORDENAMENTO JURÍDICO BRASILEIRO

Trabalho de Conclusão de Curso – Artigo – apresentado ao Curso de Direito da Universidade Tiradentes – UNIT, como requisito parcial para obtenção do título de bacharel em Direito.

Professor Júlio César do Nascimento Rabelo

Aracaju

2020

RESUMO

A presente pesquisa visa discorrer sobre o conceito, os fatos históricos e a prática dos cibercrimes, sob o viés do Código Penal Brasileiro. Devido aos grandes avanços tecnológicos que ocorreram ao longo do tempo, houve o surgimento dos cibercrimes, que são crimes praticados através da Internet ou com o auxílio dela, envolvendo condutas criminosas que violam os direitos fundamentais das pessoas. A escolha do tema em questão surgiu da necessidade de um conhecimento mais aprofundado sobre essa tecnologia que faz parte do cotidiano e dia-a-dia da maioria das pessoas de qualquer parte do mundo. A partir de estudos e análises de textos, foi realizada uma reflexão sobre os tipos de crimes cometidos por meio da Internet, visando esclarecer quem são os autores, como agem e a problemática da dificuldade na investigação e criação de uma política criminal necessária para a prevenção e correta punição dos cibercriminosos.

Palavras-chave: Cibercrimes. Internet. Código Penal Brasileiro.

ABSTRACT

This research aims to discuss the concept, the historical facts and the practice of cybercrimes, under the bias of the Brazilian Penal Code. Due to the great technological advances that have occurred over time, there has been the emergence of cybercrimes, which are crimes committed over the Internet or with the help of it, involving criminal conduct that violates people's fundamental rights. The choice of the subject in question arose from the need for a more in-depth knowledge about this technology, which is part of the daily life of most people in any part of the world. Based on studies and analysis of texts, a reflection was made on the types of crimes committed through the Internet, aiming to clarify who the authors are, how they act and the problem of the difficulty in investigating and creating a necessary criminal policy for prevention and correct punishment of cybercriminals.

Keywords: Cybercrimes. Internet. Brazilian Penal Code.

1. INTRODUÇÃO

A internet chegou ao Brasil inicialmente com acesso limitado a professores, estudantes, universidades e instituições de pesquisa. Somente alguns

anos após, as pessoas fora do âmbito acadêmico puderam ter acesso à Internet, criando um ambiente de constante troca de dados e informações em velocidade instantânea. A consequência disto foi o início de uma sociedade global, onde todos estão conectados a todo tempo, a partir de diversos meios diferentes, possibilitando as pessoas uma maior comodidade, ao poder realizar compras, fazer pesquisas, transferências de dinheiro, enviar mensagens, publicar conteúdos e até acessar uma conta bancária sem sair de casa.

Em decorrência do mais comum e fácil acesso à internet, as pessoas acabaram por tomar posturas mais descuidadas em relação à privacidade de dados, imagens e hábitos que compartilham nos diversos meios disponíveis. No entanto, ambiente integrado possibilitou também a atuação de criminosos que podem praticar todo tipo de crime e atividade ilícita por meio da internet, essas condutas ilícitas são denominadas cibercrimes, ou crimes cibernéticos.

Atualmente, é muito comum vermos notícias de invasão de celulares e computadores de empresas, personalidades do mundo político e artístico, ou até mesmo simples cidadãos. Podem ocorrer diversos tipos de crimes através da internet, desde a invasão de privacidade, espionagem, furto de informações, divulgação ilícita de imagens, conversas, documentos, até o tráfico de drogas, armas e produtos falsificados. É importante destacar, que os criminosos do mundo virtual são diferentes dos criminosos do mundo real, pois são pessoas que possuem um elevado nível de conhecimento técnico e na grande maioria das vezes agem no anonimato, utilizando tecnologias que impedem o rastreio e identificação do autor da ação, sendo possível a prática de inúmeros crimes, a qualquer momento, de qualquer local, até mesmo da sua própria casa, sendo acobertado pela dificuldade na investigação por parte das autoridades policiais.

A carência de agilidade no processo de investigação e conhecimento técnico por parte das autoridades acaba dificultando e comprometendo a eficiência do combate aos crimes cometidos por meio da internet, e acaba por gerar uma sensação de impunidade. É visível o crescente mercado ilícito na rede mundial de computadores, por isso é necessário maiores investimentos em mão de obra especializada e desenvolvimento de novas tecnologias para conseguir suprir a demanda desses casos que na grande maioria das vezes são analisados com dificuldade.

O presente trabalho tem como ideia fundamental, abordar os aspectos históricos pertinentes ao surgimento e evolução da internet, expor o conceito, modalidades e referencial teórico sobre os cibercrimes, explanar os tipos de cibercrimes mais praticados no Brasil, a Lei n° 12.737/2012, que ficou conhecida como “Lei Carolina Dieckman”, passando pelo Marco Civil da Internet, e por fim apresentar as dificuldades encontradas pelas autoridades policiais na investigação e punição desses delitos. O método de pesquisa utilizado foi à pesquisa bibliográfica.

2. ASPECTOS HISTÓRICOS DA INTERNET NO BRASIL E O USO ATUAL

2.1. História e surgimento da internet no Brasil

A internet surgiu no mundo na década de 60, desenvolvida em meados da Guerra Fria, como resultado de uma disputa de poderes pela comunicação dos Estados Unidos contra a União Soviética. No entanto, no Brasil surgiu somente na da década de 90, sendo inicialmente implantada como uma estrutura de comunicação para fins acadêmicos, possibilitando que Universidades de todos os lugares pudessem se conectar, por meio de uma rede que permitia a troca de mensagens. Isso só foi possível por conta da criação do projeto militar ARPANET da Agência de Projetos de Pesquisa Avançada dos Estados Unidos, que foi a primeira rede de computadores interativa à base de troca de dados. (CARVALHO, 2006)

A rede de troca de dados brasileira foi criada pelo Ministério da Ciência e Tecnologia e ficou conhecida inicialmente por Rede Nacional de Pesquisas (RNP), cujo objetivo era implantar uma moderna estrutura que abrangesse todo o território nacional, complementada por redes estaduais, essas custeadas com recursos das fundações estaduais de auxílio à pesquisa, sendo então, responsável por fornecer acesso à internet a aproximadamente 600 instituições. No ano de 1991, a rede de troca de dados brasileira já era denominada Internet, e seu acesso já auxiliava órgãos do governo, servindo para transferências de arquivos, debates e acesso à base de dados nacionais e internacionais. (CARVALHO, 2006)

A Internet brasileira desenvolveu-se muito rapidamente, e em 1993 já estava presente em grande parte do país, cada vez mais acessível. Nesse mesmo ano, o Canal Vip foi o primeiro sistema brasileiro a oferecer uma conta de e-mail

gratuita, a qualquer pessoa, por meio do BBS (Bullet Board System) que era um sistema que permitia as pessoas se conectarem via telefone, possibilitando a troca de arquivos, mensagens e fotos. Nos anos seguintes, a Internet caiu nos agrados da sociedade, todos passaram a comentar e a cada vez mais querer fazer parte desse novo mundo, dando início a um processo de divulgação dos seus benefícios entre a população, estudantes e empresas.

Dois anos após, no ano de 1994 os primeiros sites foram criados pelos alunos da USP, e como conseqüência, a internet passou a ser comercializada pela empresa de telecomunicação Embratel. Somente no ano seguinte foi realizada a primeira transmissão ao vivo entre estados, realizada por São Paulo e Rio Grande do Sul. Ainda em 1995, houve a criação do Comitê Gestor da Internet no Brasil, com o objetivo de coordenar todas as iniciativas de serviços de Internet no país, pois o Ministério das Telecomunicações em conjunto com o Ministério da Ciência e Tecnologia começaram a disponibilizar o acesso à internet para toda a população. (KLEINA, 2018)

No ano de 1996, a internet já estava amplamente consolidada na sociedade e com isso surgiram os primeiros portais de internet privados do Brasil, como o UOL. A novidade chamada Internet chegou a virar capa da revista Veja e até tema da novela Explode Coração, que relatava o amor virtual de um casal que se comunicavam por meio de vídeo chamada através da Internet. Ainda no mesmo ano, o cantor Gilberto Gil fez a primeira transmissão musical via Internet, lançando a música intitulada Pela Internet e conversou com internautas. (KLEINA, 2018)

Os provedores de acesso só surgiram no ano 2000, em um primeiro momento através de conexão discada, sendo financiadas por meio de propagandas expostas nos navegadores, porém o modelo se tornou insuficiente, pois no mesmo ano, surgiram os primeiros provedores de acesso através da banda larga, que possuíam uma maior qualidade de conexão e permitiam pela primeira vez a transmissão de vídeo, deixando para trás os provedores de acesso por conexão discada. (KLEINA, 2018)

A banda larga trouxe novas possibilidades e avanços para o usuário da Internet no Brasil, tendo em vista sua melhor qualidade de conexão. As falhas no

acesso à rede e as quedas de conexão diminuíram, sendo possível, portanto, acessar conteúdos com mais facilidade, como fotografias, músicas, filmes, sem qualquer desconforto, dando início a novas funções e meios de utilização de uma internet mais moderna.

2.2. Uso moderno da Internet

Com os constantes avanços da internet, surgiram às redes sociais no ano de 2004, as principais foram primeiramente o Orkut e posteriormente o Facebook. Essas redes sociais permitiram as pessoas trocarem mensagens instantaneamente, publicarem fotos, vídeos ou textos sobre o que estavam pensando, inclusive buscar o perfil de outras pessoas de qualquer parte do mundo sem precisar sair de casa. Foi nessa mesma época que as pessoas começaram a criar o hábito de conectarem seus computadores à internet com mais frequência, passaram a acompanhar todas as notícias que ocorriam no mundo e a interagir em comunidades e fóruns nas redes sociais, deixando de lado as mídias tradicionais como o jornal e rádio. (KLEINA, 2018)

A partir daí, a Internet começa a se desenvolver muito rápido, e o surgimento dos smartphones e da conexão 3G, disponível para os aparelhos móveis, trouxeram mais facilidade e agilidade no acesso das pessoas ao mundo virtual. O surgimento dos smartphones causou uma revolução mundial e consolidou a Internet na vida cotidiana das pessoas, que passou a ser vista como uma ferramenta essencial no dia a dia, tendo em vista que a tecnologia possibilitou um acesso mais rápido e independente, já que o usuário passou a acessar a internet de qualquer lugar a qualquer hora, não necessitando estar em frente a um computador, em um local fixo. (RUTHERFORD, 2015)

Entre as diversas funções da internet, os usuários podem realizar compras, chamadas de vídeo, transferência de diversos arquivos, acesso à conta de e-mail, sendo possível até gerenciar uma conta bancária. As empresas também foram beneficiadas, diminuíram sua mão-de-obra ao substituírem seus funcionários que trabalhavam em lojas físicas e passaram a dispor de novas formas de fazer negócio, através de sites, aplicativos, publicidades online ou nas redes sociais, com

isso, tiveram um aumento na visibilidade e venda dos seus produtos, pois não era mais necessário alguém se deslocar da segurança da sua casa até uma loja em um local fixo para consultar a disponibilidade de um produto e realizar a compra, podendo fazer tudo isso através do meio virtual.

2.3. Noções gerais sobre os crimes cibernéticos

Em decorrência das facilidades que os avanços tecnológicos trouxeram para toda a população, cada vez mais pessoas se conectam a Internet diariamente, seja para realizar qualquer tipo de serviço com mais agilidade e praticidade, ou somente para trocar mensagens e interagir em redes sociais. No entanto, muitas das vezes acabam inserindo seus dados, endereço, e até senhas bancárias ou de cartões, em troca de serviços, informações, possíveis cursos ou compras virtuais, dentre muitas outras possibilidades ofertadas em troca das informações dos usuários da rede. Por consequência, os usuários tornam-se vulneráveis e podem ser vítimas de possíveis crimes virtuais, uma prática que torna-se cada vez mais comum no Brasil, e por isso, é de extrema importância ter o mínimo conhecimento de como funcionam esses crimes, para fazer um uso mais seguro da Internet.

Não há dúvidas de que a Internet é uma ferramenta muito útil em todas as áreas da vida das pessoas, seja nas atividades laborais, acadêmicas, nos afazeres da vida cotidiana, já que é possível, por exemplo, ter maior parte das necessidades diárias atendidas através de serviços que podem funcionar de *home Office*, cursos de toda variedade, aplicativos de delivery, dentre inúmeros outros serviços disponíveis. No entanto, a despeito de tantos benefícios que a tecnologia proporciona, há também os os ônus do uso de forma imprudente ou inexperiente, podendo causar transtornos na vida de alguém, caso este venha ser vítima de um crime virtual.

As pessoas devem saber que as novas possibilidades que o ambiente virtual trouxe, facilitou também a atuação de criminosos, além de criar novas modalidades de atividades ilícitas, portanto, a maioria da população mundial que usam aparelhos conectados a Internet já tiveram algum contato com alguma informação a respeito dos crimes virtuais e com as consequências imputadas às

vítimas desses criminosos. Em virtude das lesões de diversos tipos, sejam elas financeiras, morais ou outras, as pessoas que desconhecem os perigos e riscos do uso diário da Internet sem o devido conhecimentos das possibilidades criminosas, devem ser informadas a fim de evitar tornarem-se vítimas de tais delitos. Afinal, com esse crescimento desacelerado do acesso a Internet, também houve crescimento dos problemas resultantes da sua utilização inconsciente. (D'URSO, 2019)

Primeiramente para uma maior proteção contra os cibercrimes, é preciso conhecer os tipos de criminosos que atuam na Internet, os tipos de crimes existentes e o modo como eles são executados. Pode-se tomar como exemplo, a utilização de ferramentas que possibilitam fazer edição de fotos, além da invasão da privacidade dos usuários, havendo o roubo de dados dos seus celulares ou computadores, sendo esses os crimes mais comuns e que mais tem impacto na vida das pessoas. (RUTHERFORD, 2015)

Ao furtar as informações de uma pessoa, os criminosos passam-se por ela, cometendo assim, o crime de falsidade ideológica, tendo como objetivo a prática de atividades ilícitas, como alterar a senha de cartões de crédito para uso indevido, invasão dos e-mails para obtenção de informações sigilosas, compartilhamento das informações alheias obtidas ilegalmente, entre outras várias possibilidades de crimes que podem ser cometidos. Os cibercimes não se restringem apenas ao furto ou invasão de privacidade, existem vários outros tipos que são cometidos até por pessoas comuns, não necessitando ter um conhecimento técnico elevado, entre eles existem a calúnia, difamação, tráfico, pedofilia, crimes que muitas das vezes não são consumados na Internet, mas toda a preparação é feita através dela. Como exemplo, o crime de estelionato na internet, se inicia com o roubo de informações pessoais da vítima através de dispositivo eletrônico, e se consuma com o uso ilícito dessas informações roubadas.

Devido ao crescente histórico de atividades ilícitas praticadas através da Internet, é de extrema necessidade haver uma atualização na regulamentação desses casos que na grande maioria das vezes são enquadrados como atípicos e julgados com muita dificuldade por conta da falta de legislação específica do nosso Ordenamento Jurídico, fato que já era esperado, pois a Internet surgiu após a

promulgação da Constituição Federal, sendo impossível a criação de uma regulamentação daquilo que não se conhecia na época. (RUTHERFORD, 2015)

3. CLASSIFICAÇÃO DOS AUTORES DOS CRIMES CIBERNÉTICOS

Os cibercrimes são cometidos por criminosos que se aproveitam da falta de conhecimento técnico das pessoas para invadirem sua privacidade e obterem as mais diversas informações, sendo possível a prática dos mais variados tipos de crimes e atos ilícitos. Ao falar em práticas criminosas no meio virtual, as pessoas usam o termo hacker de forma genérica, na maioria das vezes por não conhecer a diferença entre os conceitos de hacker e craker. Ocorre que os dois conceitos servem para denominar pessoas que possuem habilidades elevadas com computadores e Internet, porém, cada um usa suas habilidades para fins diferentes. (RUTHERFORD, 2015)

3.1. Hacker

O conceito Hacker teve origem da língua inglesa e era usado para definir as pessoas que tinha um considerável conhecimento técnico sobre aplicativos, programas e redes de computadores. Com a popularização dos computadores, a mídia passou a usar o termo hacker para definir os autores dos crimes no meio virtual, por isso a grande parte da população passou a associar o termo à prática de fatos criminosos. (MARINHO, 2016)

Ocorre que os Hackers são pessoas com um alto grau de conhecimento e habilidades de programador que o permitem invadir sistemas, porém sem destruí-lo e sem obter dados. Muitos desses são contratados por empresas para cuidar da sua segurança, descobrir falhas nos sistemas e desenvolver novas formas de proteção, para evitar o ataque de criminosos virtuais, ou seja, eles utilizam seus conhecimentos para o bem, são profissionais com ética e não criminosos como são vistos pela maioria da população.

3.2. Cracker

Por falta de informação, a maioria das pessoas acha que os Hackers são os verdadeiros criminosos, considerando fato de possuírem conhecimentos sobre segurança e sistemas, o que de fato ocorre, todavia, esses não são utilizados para práticas ilegais, diferente dos verdadeiros autores dos cibercrimes, que são denominados Crackers. O conceito de Cracker foi criado pelos próprios Hackers, que tinham como objetivo educar a mídia e a sociedade para que não fossem confundidos com as pessoas que praticavam os cibercrimes. Portanto, os Crackers são pessoas que decifram códigos de proteção de forma ilegal, favorecendo a pirataria, além de invadirem os sistemas para roubar informações e causar danos às vítimas, ou seja, são criminosos virtuais que usam seus conhecimentos para quebrar proteções virtuais e senhas, e com isso ganhar dinheiro vendendo as informações roubadas. (RUTHERFORD, 2015)

Os crackers almejam ganharem dinheiro e fama ao roubarem dinheiro, cartões de crédito, informações confidenciais, contas bancárias, dados pessoais e outras informações valiosas, subornando as vítimas com as informações roubadas. Por ter um elevado nível de conhecimento técnico, é muito difícil identificar os autores dos crimes, pois eles atualizam suas técnicas a cada dia que passa. Há casos em que os Crackers acabam sendo presos, porém, na maioria das vezes o dinheiro ou dados roubados não são recuperados. (AMARIZ, 2014)

4. CLASSIFICAÇÃO DOS MALWARES MAIS USADOS NOS CRIMES CIBERNÉTICOS

O conceito de vírus surgiu em meados dos anos noventa, anteriormente ao termo malware, quando os programas maldosos começaram a se tornarem mais comuns. Ao se falar em ameaças digitais, é comum ouvir os termos vírus e malware, porém eles não são sinônimos, pois todo vírus é um malware, mas nem todo malware é um vírus. (GARRETT, 2018)

O conceito de malware surgiu a partir da junção do termo “malicioso” com “software”, portanto, malware é usado para se referir a qualquer programa de computador ou celular que seja capaz de se instalar ou se reproduzir sozinho,

gerando danos e realizando ações indesejadas nos aparelhos afetados. Em suma, o malware é um tipo de software maligno que invade a privacidade das pessoas, acessando os aparelhos das pessoas sem que elas saibam. (GARRETT, 2018)

O vírus se destingue do malware, pois o vírus não tem a capacidade de se reproduzir ou se instalar sozinho, ele necessita que o usuário venha a abrir um arquivo ou link infectado. Portanto, o termo malware é correto para definir todos os tipos de softwares maliciosos, incluindo os vírus.

4.1. Adware

O Adware é um dos malwares mais incômodos e repetitivos do mundo virtual, pois envia diversos anúncios automaticamente para os dispositivos dos usuários. Geralmente, pode contaminar o aparelho do usuário através de anúncios pop-up em páginas virtuais e publicidades dentro de programas, que direciona o usuário para algum tipo de benefício gratuito. Após ser instalado, o Adware é capaz de rastrear o aparelho do usuário para coletar informações de localização e navegação online, rastreando todas as atividades do usuário para descobrir qual publicidade deverá direcionar, reduzindo o desempenho do aparelho. (MARTINS, 2008)

Devido a grande quantidade de anúncios e propagandas enviadas, o cibercriminoso acaba ganhando dinheiro por cada clique realizado nos anúncios exibidos, além de venderem a terceiros, os dados de navegação e localização roubados dos usuários que foram contaminados pelo Adware. Por isso, os usuários devem tomar cuidados especiais com sites falsos, e-mails desconhecidos, downloads de arquivos e fontes inseguras, e o mais importante, não acessar propagandas e anúncios maliciosos.

4.2. Cavalo de Tróia

O nome Cavalo de Troia dado ao malware teve influência na Grécia antiga, a técnica usada pelo povo grego é a mesma usada atualmente para contaminar os aparelhos das pessoas. Assim caracterizado pois o malware finge ser

um programa inofensivo, para fazer com que seja instalado e com isso ter a possibilidade de acessar os aparelhos das pessoas, espioná-las e até roubar, excluir ou modificar seus dados, com isso, o Cavalo de Troia se tornou um dos malwares mais populares entre os criminosos online. (REGAN, 2019)

Este tipo de malware não tem capacidade de se reproduzir sozinho, sua função é fazer mudanças na proteção e segurança dos aparelhos, para facilitar a instalação de outros malwares escondidos. Portanto, os Cavalos de Troia permanecem ocultos, aguardando que o usuário acesse suas contas bancárias ou insira dados do seu cartão de crédito, para ter o controle do aparelho, enviar senhas e outros dados ao criminoso e até impedir o acesso do usuário.

4.3. Rootkits

O Rootkit é um malware malicioso que tem como função principal ocultar determinados arquivos e processos específicos em partes do dispositivo, passando a fornecer aos cibercriminosos acesso e controle do dispositivo para roubar dados ou instalar outros malwares, sem o consentimento do usuário. (BELCIC, 2020)

Geralmente, os Rootkits se integram ao sistema operacional, se passando por um componente essencial e benéfico, em conseqüência dessa camuflagem os antivírus não conseguem detecta-lo como uma ameaça, enganando os sistemas de proteção e detecção menos avançados. Passa, portanto, a estender o seu período de atividade nos computadores ou celulares infectados, diminuindo o desempenho e provocando falhas nos comandos e até mudanças nas configurações.

Os Rootkits se instalam a partir de brechas no sistema de dispositivos que não foram atualizados, ou através de links maliciosos que podem ser enviados em redes sociais, e-mails desconhecidos ou aplicativos e arquivos baixados em fontes não confiáveis. Assim, para uma maior proteção, é importante não baixar arquivos desconhecidos, verificar se o sistema está devidamente atualizado, realizar a instalação de um bom antivírus, e tomar cuidados ao inserir pen drives de terceiros

4.4. Spyware

O Spyware é um tipo de malware que se infiltra nos computadores ou smartphones, com o objetivo de espionar todas as ações realizadas pelo usuário, para coletar informações pessoais ou confidenciais de forma ilegal e transmiti-las para terceiros através da Internet, sem a permissão ou consentimento do usuário. Este tipo de Malware se difere dos Cavalos de Troia, pois não almejam o domínio ou manipulação do sistema do usuário, seu objetivo é apenas espionar e roubar informações ilegalmente, rastreando os hábitos de navegação, senhas pessoais e comportamento do usuário no meio virtual. (SOUZA, 2020)

Quase todos os Spywares são maliciosos, criados para monitorar e coletar informações confidenciais para serem usadas na prática de atividades ilegais. Porém, alguns não são maliciosos, é o caso das empresas comerciais e de anúncios, que utilizam Spywares de forma legal, coletando informações de seus usuários com o consentimento dos mesmos, para filtrar os anúncios que irão apresentar. Ocorre que nem todas as empresas utilizam os Spywares de forma legal, algumas usam para monitorar os hábitos e costumes dos usuários, sem que eles saibam, e posteriormente vender todos os dados para cibercriminosos, que praticam todo tipo de atividade ilícita, prejudicando o usuário afetado.

4.5. Worms

Os Worms significam Vermes, são Malwares com elevada capacidade de se replicarem sem o controle e consentimento do usuário, criando cópias adicionais de si mesmo por toda parte do sistema, sendo quase impossível removê-lo completamente. (POZZEBOM, 2015)

Este Malware se replica muito rápido e contamina outros dispositivos, através da Internet, mensagens, e-mails e Drivers USB. As mensagens e e-mails são enviados automaticamente, contendo links maliciosos para infectar outros aparelhos, por isso, é muito difícil ser reconhecido pelos usuários, pois as mensagens são de contatos e e-mails de pessoas conhecidas, que já estão infectadas. Portanto, é necessária uma atenção maior ao receber e-mails suspeitos e arquivos de procedência desconhecida.

5. A LEGISLAÇÃO E O COMBATE AOS CRIMES CIBERNÉTICOS

A Constituição Federal prevê em seus artigos a garantia de diversos direitos, porém muitos desses direitos são violados na internet. Muitas pessoas acham que essa impunidade é devido à falta de regulamentação específica no âmbito penal, facilitando a prática de crimes através do meio virtual.

5.1. Lei 12.737/2012, Lei Carolina Dieckman

Popularmente conhecida como Lei Carolina Dieckman, a Lei 12.737/12 surgiu após a atriz brasileira ter sido vítima de invasão de privacidade. Os criminosos roubaram fotos e conversas íntimas e pediram dinheiro para que não divulgassem sua intimidade na internet.

Antes da referida lei ser criada, a dificuldade na tipificação dos cibercrimes era muito grande. Sua vigência representou um grande avanço com relação aos crimes praticados por meio da internet, pois foi a primeira lei brasileira criada exclusivamente para tipificar cibercrimes, expressando que a conduta de invadir dispositivo informático passou a ser considerada crime, além de prever causas de aumento de pena e crimes equiparados. (BARRETO, 2017)

Ocorre que a Lei Carolina Dieckman não é totalmente eficaz, pois prevê que é necessária a violação do dispositivo de segurança para ocupação ou como forma de conquista de modo abusivo para a conduta ser enquadrada como crime, quando na verdade, o ideal seria tipificar como crime a mera conduta de invasão ilegal do dispositivo alheio. Além disso, a referida lei usa o termo “dispositivo informático”, termo esse que não abrange todos os tipos de aparelhos que possuem acesso à internet e consequentemente podem sofrer esse e outros tipos de cibercrimes. Outro ponto frágil dessa lei é que a pena estabelecida não é suficiente para reprimir as condutas criminosas, além de não haver previsão dos outros diversos tipos de crimes que são praticados através da internet. (NASCIMENTO, 2019)

5.2. Marco civil da internet

Desde a promulgação da atual Constituição até o ano de 2012 só existiam algumas leis que previam a proteção dos dados, não havia nenhuma lei que tipificava exclusivamente os delitos cometidos por meio da Internet, portanto esses delitos eram punidos com base no resultado das ações. (CRUZ; RODRIGUES, 2018)

O Marco Civil surgiu para disciplinar o uso da internet no Brasil, garantir direitos aos seus usuários, como liberdade de expressão, de comunicação, proteção de dados pessoais, privacidade, inclusive acesso para qualquer pessoa, sem distinção, pois expressa que o acesso à internet é essencial ao exercício da cidadania e todos devem ter acesso à informação, ao conhecimento e as inovações tecnológicas.

O novo amparo legislativo foi visto como a Constituição Federal da Internet, e além de garantir direitos aos usuários, trouxe amparo aos provedores de conexão de internet, que são aquelas empresas que fornecem o acesso à conexão, prevendo a isenção de responsabilidade civil por danos decorrentes de conteúdo gerado por terceiros. Os provedores de aplicação, que são as empresas que fornecem os serviços online, como sites, e-mails e redes sociais, só serão responsabilizadas por danos decorrente de conteúdo gerado por terceiros, se o conteúdo for constatado ilícito e após ordem judicial determinada, não tomar as devidas providências dentro do prazo legal. (BRASIL, 2019)

Um dos principais benefícios que o Marco Civil trouxe foi o princípio da neutralidade da rede, que tem como objetivo impedir que empresas prestadoras de serviços de internet e telefonia limitem o acesso e os serviços dos seus usuários, definindo essa prática como abusiva. Outro princípio muito importante é o princípio da privacidade, que garante a inviolabilidade das comunicações feitas entre os usuários e sigilo das informações pessoais, além de prever que a quebra do sigilo só pode ocorrer mediante ordem judicial, quando tal medida for necessária para solucionar casos de cibercrimes e identificar os autores. (CRUZ, 2019)

5.3. Dificuldades na investigação dos crimes cibernéticos

Com a entrada em vigor do Marco Civil da Internet, os cibercrimes passaram a receber uma maior atenção por parte das autoridades policiais e o número de investigações envolvendo esses delitos online cresce cada vez mais.

O fato é que ainda existem alguns problemas que dificultam a investigação por parte das autoridades policiais, como por exemplo, a falta de mão de obra especializada e desenvolvimento de novas tecnologias que auxiliem na busca dos autores, pois deve haver investimentos e preparos para conseguir suprir a demanda, até porque o número de cibercrimes supera o número de agentes capacitados para realizar investigações. O ordenamento jurídico brasileiro prevê que a sanção penal só poderá ser aplicada quando for comprovada a autoria e materialidade do crime, sendo fundamental a existência de provas obtidas por meios lícitos, caso contrário o Juiz poderá absolver o réu. (CRUZ; RODRIGUES, 2018)

Um dos principais problemas que dificulta e atrasa o processo de investigação dos cibercrimes é que na maioria das vezes a autoridade policial ao identificar a forma como o crime ocorreu e o local que ocorreu, necessita de uma autorização judicial para realizar comunicações com as empresas que armazenam informações dos dispositivos usados pelos cibercriminosos. Só após todo esse trâmite processual demorado, as autoridades policiais poderão ter acesso às informações e identificar o autor. (CRUZ; RODRIGUES, 2018)

6. CLASSIFICAÇÃO DOS CIBERCRIMES MAIS PRATICADOS

Atualmente, todo o mundo está conectado através da Internet, se tornou algo essencial que está presente na vida da maioria das pessoas diariamente. Com todas as facilidades que a Internet proporciona, as pessoas passaram a realizar suas atividades no meio virtual, como por exemplo, pagar boletos, fazer transações financeiras e até compras em lojas online, para isso é preciso fornecer dados de contas bancárias, cartões de crédito ou débito e dados pessoais.

Devido ao elevado número de usuários acessando a Internet a todo o momento para desempenhar as mais variadas atividades, há cada vez mais cibercriminosos visando obter lucro e tentando cometer algum tipo de crime, seja

roubar alguma informação, instalar algum vírus, entre vários outros crimes, que na grande maioria dos casos não há definição penal específica. A seguir serão explanados alguns dos cibercrimes mais praticados no Brasil.

6.1. Crimes de furto e estelionato

Um dos cibercrimes que ocorrem com bastante frequência no meio virtual é o furto, seja de dados da vítima, senhas bancárias, informações sigilosas de empresas. Ocorre que o roubo de qualquer coisa através da internet, na maioria das vezes é enquadrado como estelionato e definido da seguinte forma pelo artigo 171 do Código Penal: Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento. (LOPES, 2017)

O crime de furto e estelionato através da internet, na maioria das vezes estão ligados um ao outro, pois geralmente o cibercriminoso rouba dados de cartões para se passarem pela vítima e posteriormente efetuar compras e extrair dinheiro de contas bancárias. O roubo de identidade no ordenamento jurídico brasileiro encontra-se no artigo 307 do Código Penal: Atribuir-se ou atribuir à terceiro, falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem.

6.2. Crimes contra a honra (Injúria, Difamação e Calúnia)

Assim como o crime de discriminação, os crimes de injúria, difamação e calúnia se tornaram muito comuns na internet, pelo fato das pessoas acharem que não serão punidas pelos atos praticados no mundo virtual. O principal ambiente onde as ofensas ocorrem são as redes sociais, local onde as pessoas podem fazer comentários, compartilhar textos, fotos e vídeos livremente. É muito comum ocorrer divergências de opiniões que levam a discussões, com isso, algumas pessoas ultrapassam os limites do bom senso, fazem falsos comentários, ofendem a honra, e prejudicam a reputação das outras pessoas, ferindo seus direitos.

A depender da gravidade das ofensas, o procedimento recomendado é a vítima imprimir as ofensas como meio de prova e fazer uma denúncia para que o fato seja averiguado, podendo ser passível de danos morais. Portanto, mesmo este crime ocorrendo através da internet, serão aplicadas as normas já existentes no Código Penal, mais especificamente os artigos 138, 139 e 140 do referido código. (RUTHERFORD, 2015)

6.3. Crime de discriminação

Como já foi exposto anteriormente, a Internet é utilizada por milhares de pessoas diariamente, que podem expressar suas opiniões em questão de segundos, por conta disso, é muito comum ocorrer situações envolvendo a prática do crime de discriminação, tanto racial, como de gênero. Muitas pessoas acham que a Internet é um ambiente anônimo, que podem postar e comentar o que quiserem, e até mesmo ferir os direitos de outra pessoa, sem haver qualquer consequência ou punição. Porém a Internet não é um ambiente sem lei, e atualmente, as leis do Código Penal também se aplicam no mundo virtual, mesmo porque os cibercrimes causam o mesmo dano que os crimes praticados no mundo real, ou até maiores, se consideradas a repercussão e alcance característicos da rede.

Qualquer pessoa que for vítima de discriminação, seja ela de qualquer tipo, pode denunciar o crime anonimamente às autoridades especializadas na investigação e aplicação das leis no combate aos crimes que ferem os direitos humanos no meio virtual. Caso a denuncia se concretizar verdadeira, quem for acusado de discriminação racial, religiosa, de gênero ou qualquer outra na internet, poderá ser condenado a pena de reclusão de dois a cinco anos e multa. (CAMPOS, 2017)

6.4. Incitação e apologia ao crime

A internet se tornou um local onde qualquer pessoa de qualquer lugar do mundo pode livremente expressar sua opinião e acessar as mais variadas informações. É comum haver páginas e perfis que estimulam a prática de delitos criminosos, geralmente são privados e restritos aos participantes que compartilham

experiências na prática de crimes, incentivam a prática e tentam recrutar novos membros, tudo isso porque a internet é vista pela maioria das pessoas como um ambiente sem lei. (RUTHERFORD, 2015)

Caso uma denúncia de divulgação de vídeos, comentários ou compartilhamentos que apoiam a violência ou o crime venha a se concretizar verdadeira, o fato se enquadrará no artigo 287 do Código Penal: “Fazer, publicamente, apologia de fato criminoso ou de autor de crime: Pena - Detenção, de três a seis meses, ou multa”. Portanto, o ato de estimular a prática de crimes de forma pública ou defender algum fato criminoso, ambos se enquadraram na mesma tipicidade penal.

6.5. Pirataria

Devido à velocidade de compartilhamento de arquivos na internet, é muito comum haver crimes que violam direitos à propriedade intelectual, literária, artística e industrial. Com isso, surge o crime de Pirataria, que é mais conhecido como Pirataria Digital, onde os criminosos se utilizam de métodos específicos para realizar a cópia ilegal de vários tipos de arquivos, filmes, jogos, programas e principalmente conteúdos pagos, gerando muitos danos.

Os criminosos costumam copiar jogos, livros, músicas, shows originais, e disponibilizar gratuitamente para download na internet. Outra prática bastante comum é a criação de sites e aplicativos piratas que reproduzem filmes, séries, canais fechados e conteúdos pagos de forma ilegal. O conteúdo dos sites piratas é obtido ilegalmente e vendido para terceiros, com isso, os criminosos ganham dinheiro vendendo assinaturas e conteúdos pagos, abaixo do valor normal e também ganham dinheiro com publicidades e propagandas de outros sites, expostas nos sites e aplicativos piratas. Portanto, a prática de obter lucro sem a autorização de quem tem os direitos sobre o conteúdo se enquadrará no artigo 184 do Código Penal, com a pena podendo chegar até quatro anos de reclusão. (GALANTE, 2019)

7. Considerações finais

O número de crimes cibernéticos está aumentando cada vez mais, e esses estão ocorrendo com maior frequência que os crimes no mundo real, sem, todavia, haver uma punição proporcional dos infratores pela prática dos seus atos criminosos. É de suma importância que as pessoas tenham conhecimento sobre os crimes que ocorrem na internet, como ocorrem e quem os pratica, portanto, o presente trabalho tem como objetivo evidenciar os principais aspectos históricos da internet nacional, expor fatos importantes sobre como ocorrem os crimes cibernéticos, a insuficiência do ordenamento jurídico brasileiro e os problemas técnicos na investigação desses delitos.

Primeiramente foram expostos aspectos históricos pertinentes à internet, os crimes cibernéticos e as diferenças conceituais entre hacker e cracker, a fim de proporcionar maior conhecimento técnico ao trabalho. Logo após, foram classificados os malwares mais utilizados pelos criminosos e como agem, explicando como as vítimas são atingidas. Em seguida foi exposta a criação de legislações importantes, como a Lei Carolina Dieckmann e o Marco Civil da Internet que estabeleceu garantias, direitos e deveres, regulando o uso da internet no Brasil, e por fim foram apresentadas as dificuldades encontradas no combate aos crimes cibernéticos e as modalidades de crimes que são mais comuns.

Independente dos crimes serem praticados na internet ou através dela, o objetivo é o mesmo que os delitos cometidos no mundo real, por isso é possível punir os infratores com base nas normas existentes, evidenciando que a maior problemática não é a falta de leis específicas e sim a dificuldade na investigação e punição dos autores desses crimes. É necessário investimentos do governo para aperfeiçoar as investigações e enfrentar as vulnerabilidades, acompanhando as evoluções tecnológicas, bem como atenção redobrada por parte da população, pois as consequências vão além do mundo virtual, na maioria das vezes, atingem a vida íntima das pessoas e geram complicações que poderão se estender por um longo período.

REFERÊNCIAS:

AMARIZ, Luiz. Hackers e Crackers. Disponível em: <https://www.infoescola.com/informatica/hackers-e-crackers/>. Acesso em: 20 fev. 2020.

BARRETO, Erick. Crimes cibernéticos sob a égide da Lei 12.737/2012. Disponível em: <https://ambitojuridico.com.br/edicoes/revista-159/crimes-ciberneticos-sob-a-egide-da-lei-12-737-2012/>. Acesso em: 5 mar. 2020.

BELCIC, Ivan. Rootkits explicados: O que fazem, como funcionam e como removê-los. Disponível em: <https://www.avast.com/pt-br/c-rootkit>. Acesso em: 29 fev. 2020.

BRASIL, Rafael. Marco Civil da Internet e responsabilidade civil no ambiente digital. Disponível em: <https://blog.sajadv.com.br/responsabilidade-civil-marco-civil-da-internet/>. Acesso em: 13 mar. 2020.

CAMPOS, Lorraine. Internet x preconceito. Disponível em: <https://vestibular.brasilescola.uol.com.br/blog/internet-x-preconceito.htm>. Acesso em: 21 mar. 2020.

CARVALHO, Marcelo. A trajetória da internet no Brasil: Do surgimento das redes de computadores à instituição dos mecanismos de governança. Disponível em: <https://www.cos.ufrj.br/uploadfile/1430748034.pdf>. Acesso em: 9 fev. 2020.

CRUZ, Carlos. Marco Civil da Internet: O que é e o que muda para o seu negócio. Disponível em: <https://chcadvocacia.adv.br/blog/marco-civil-da-internet/>. Acesso em: 15 mar. 2020.

CRUZ, Diego; RODRIGUES, Juliana. Crimes cibernéticos e a falsa sensação de impunidade. Disponível em: <http://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/iegWxiOtVJB1t5C_2019-2-28-16-36-0.pdf>. Acesso em: 9 mar. 2020.

D'URSO, Luiz. Em tempos de cibercrimes. Disponível em: <https://www.migalhas.com.br/depeso/310551/em-tempos-de-cibercrimes>. Acesso em: 12 fev. 2020.

GALANTE, Vitor. Como aplicativos gratuitos ganham dinheiro? Disponível em: <https://usemobile.com.br/aplicativos-gratuitos-ganham-dinheiro/>. Acesso em: 22 mar. 2020.

GARRETT, Filipe. Qual a diferença entre vírus e malware? Disponível em: <https://www.techtudo.com.br/noticias/2017/11/qual-a-diferenca-entre-virus-e-malware.ghtml>. Acesso em: 22 fev. 2020.

KLEINA, Nilton. Como tudo começou: A história da internet no Brasil. Disponível em: <https://www.tecmundo.com.br/mercado/129792-tudo-comecou-historia-internet-brasil-video.htm>. Acesso em: 9 fev. 2020.

LOPES, Rénan. Delitos virtuais praticados na sociedade da informação. Disponível em: <http://www.rkladvocacia.com/delitos-virtuais-praticados-na-sociedade-da-informacao/>. Acesso em: 17 mar. 2020.

MARINHO, Guilherme. Hackers, Crackers e o Direito Penal. Disponível em: <https://grmadv.jusbrasil.com.br/artigos/407334629/hackers-crackers-e-o-direito-penal>. Acesso em: 15 fev. 2020.

MARTINS, Elaine. O que é Adware? Disponível em: <https://www.tecmundo.com.br/spyware/271-o-que-e-adware-.htm>. Acesso em: 24 fev. 2020.

NASCIMENTO, Samir. Cibercrime: Conceitos, modalidades e aspectos jurídicos-penais. Disponível em: <https://ambitojuridico.com.br/cadernos/internet-e-informatica/cibercrime-conceitos-modalidades-e-aspectos-juridicos-penais/>. Acesso em: 7 mar. 2020.

POZZEBOM, Rafaela. Diferença entre: vírus, spam, spyware, worm, phishing, botnet, rootkit. Disponível em: <https://www.oficinadanet.com.br/post/12991-diferenca-entre-virus-spam-spyware-worm-phishing-botnet-rootkit>. Acesso em: 3 mar. 2020.

REGAN, Joseph. O que é um Cavalo de Tróia? É malware ou vírus? Disponível em: <https://www.avg.com/pt/signal/what-is-a-trojan>. Acesso em: 27 fev. 2020.

RUTHERFORD, Mikhail. Crimes na internet: Falta de normatização, dificuldades na regulamentação e entendimentos sobre o assunto. Disponível em: <https://mikhail.jusbrasil.com.br/artigos/234313175/crimes-na-internet-falta-de-normatizacao-dificuldades-na-regulamentacao-e-entendimentos-sobre-o-assunto>. Acesso em: 11 fev. 2020.

SOUZA, Thais. Spyware: O software espião. Disponível em: < https://ostec.blog/geral/spyware-espiao>. Acesso em 3 mar. 2020.