CIBERCRIMES: ASPECTOS PANORÂMICOS DOS CRIMES INFORMÁTICOS MAIS PRATICADOS E AS CONDUTAS DE PREVENÇÃO [1]

CYBERCRIMES: MOST COMMON CRIMES AND PREVENTION

Letícia Lourenço Sangaleto Terron[2]
Rodrigo Antônio Correa[3]
Thiago Martins Correia[4]

RESUMO

O presente trabalho possui como objetivo principal analisar a evolução dos crimes cometidos por meio eletrônico diante do crescimento da tecnologia e de seus mais diversos recursos que vem deixando os seres humanos cada vez mais dependentes do mundo virtual. Com o crescimento dos mecanismos informáticos surgiram diversificadas formas de cometimento de delitos virtuais, além de se tornar mais comum a prática dos crimes convencionais. Para obter uma conclusão e construir resultados e respostas acerca da problemática exposta neste estudo foi desenvolvida pesquisa explicativa, por meio da abordagem do método dedutivo, com a finalidade de esclarecer as causas e os efeitos dos crimes virtuais mais praticados. Partindo de pesquisa bibliográfica, pode-se reunir dados nos quais o estudo foi baseado. Como a finalidade é mostrar os mais diversificados crimes cometidos por meio eletrônico e quais formas de prevenção, a menção de trabalhos já existentes contribuiu para a construção qualitativa para o resultado do trabalho. Como resultado buscou-se evidenciar como agem os cibercriminosos e como agir diante de um cibercrime.

PALAVRAS-CHAVE: Cibercrime. Crime Virtual. Segurança da Informação. Prevenção.

[1] Artigo submetido em 22-04-2020 e aprovado em 23-05-2020.
[2] Doutoranda em Direito. Mestre em Direito. Docente do Centro Universitário de Santa Fé do Sul. Endereço eletrônico: leticiasanga@bol.com.br.
[3] MBA em Direito e Gestão Educacional. Advogado. Docente do Centro Universitário de Santa Fé do Sul. Endereço eletrônico: rodrigo_jao@hotmail.com.
[4] Graduado em Sistemas de Informação pelo Centro Universitário de Jales. Pós-Graduado em Inteligência Policial pela Faculdade Campos Elíseos. Graduando em Direito no Centro Universitário de Santa Fé do Sul. Endereço eletrônico: thiagocorreia10@gmail.com.

ABSTRACT

The main objective of this work is to analyze the evolution of cybercrimes, which are crimes committed online by using electronic communications networks and information systems. The fast rise of computer networks in modern life has created new opportunities for criminal activity, making the practice of crimes more common. In order to obtain a conclusion and create results and answers about the problems exposed in this study, an explanatory research has been developed by using the deductive method approach, aiming to explain the causes and effects of the most practiced crimes. The data to support this study has been gathered through bibliographic research. As a result, this work presents how cybercriminals may act and how to act in the face of cybercrime.

KEYWORDS: Cybercrime. Virtual Crime. Information Security. Prevention.

1. INTRODUÇÃO

Com a Era Moderna e grandes revoluções sociais surgiu a internet. A era da informação é hoje o principal atributo do mundo atual e cada vez mais o ser humano depende da tecnologia para desempenhar os afazeres do dia. Diante da globalização e da velocidade em transmitir dados e comunicação, a internet transformou-se no principal recurso utilizado hoje em dia, demonstrando que, quando bem usada, traz benefícios e novos conhecimentos. “Com esta migração e ampliação gigantesca do universo virtual e a transferência de quase tudo para a rede, devido à informatização, os criminosos também são atraídos para este ambiente, o que resulta numa migração dos crimes para a Internet.” (D’URSO, 2019). Tornou-se ambiente propício para o surgimento de diversos delitos virtuais, sob o manto aparente da não responsabilização da prática dos atos, devido ao carecimento de lei específica.

Surgiu-se o denominado cibercrime, em que os criminosos começaram a aproveitar da tecnologia para cometerem os mais diversificados delitos.

O Brasil em 2017, segundo relatório da Norton Cyber Security, passou a ser o segundo país com maiores números de casos de crimes cibernéticos. Sessenta e duas milhões de pessoas foram vítimas dos mais diversos tipos de crimes virtuais, relata a empresa.

Aprofundando no assunto, em um primeiro momento, o estudo apresenta as demasiadas formas de práticas delituosas. Pode-se notar quão extensa é a lista de crimes que são praticados por meios eletrônicos. Na etapa final, explora-se diversas maneiras de aumentar a segurança para defesa e prevenção da proteção de dados, na intenção de não sofrer golpes e crimes eletrônicos, como também ilustrou formas de agir quando tratar-se de vítima de cibercrime, visto que a quantidade de recursos e ferramentas digitais devem crescer no futuro.

Por fim, empregou-se o tipo de pesquisa explicativa, baseando-se em levantamento de informações de materiais bibliográficos, mencionando trabalhos já existentes para uma construção qualitativa, a fim de determinar, por meio da abordagem do método dedutivo, as causas e os efeitos dos crimes virtuais mais praticados e, através de pesquisa explicativa, elencar diversas formas de prevenção.

2. MARCO CIVIL DA INTERNET

A Lei nº 12. 965 de 23 de junho de 2014 é intitulada como sendo o Marco Civil da Internet (MCI) no Brasil. Propõe diretrizes para a utilização da Internet, trazendo em seu bojo diversos princípios, direitos, garantias e deveres, garantindo aos usuários proteção contra invasores e qualidade de serviço. Jair Lucio Alves Filho e Bruna Moraes Marques concluem que:

> [...] o Marco Civil da Internet veio preencher uma lacuna na legislação brasileira, pois a internet tem se tornado um ambiente cada vez mais frequentado pelos brasileiros. A regulamentação das relações sociais e das situações que envolvem o mundo virtual tem se mostrado medida que se impõe, razão pela qual a Lei n.º 12.965/14 se apresenta como norma geral que norteará a criação de diversos diplomas sobre o assunto. (FILHO, MARQUES, 2017).

O MCI, também chamado de Constituição da Internet Brasileira, foi um avanço muito importante para normatizar o uso da rede mundial de computadores. Dentre diversas conquistas, o MCI conferiu um conjunto de princípios, dos quais pode citar a proteção de dados pessoais e a privacidade, registros dos acessos, neutralidade da rede, universalidade, segurança, liberdade de expressão.

A liberdade de expressão é um dos principais princípios garantidos pela lei. Na utilização da Internet é preciso respeitar o previsto na Constituição Federal. Este direito

continua assegurado, porém, ao contrário do que se pode imaginar, os usuários podem ser responsabilizados por suas ações, por conta de que, do mesmo modo em que é assegurada a liberdade de expressão, a Carta Magna brasileira protege a pessoa ofendida pela manifestação.

Outro princípio bastante importante com o advento da lei é o da privacidade. Foi inserido como forma de garantia de segurança no acesso de informações e da inviolabilidade da intimidade da vida privada. Da mesma forma atesta o princípio dos dados pessoais, que garante proteção para os usuários ao utilizar seus dados na Internet, principalmente em compras online.

O princípio da neutralidade assegura que as informações realizadas na Internet não podem ser tratadas com discriminações. As informações devem trafegar na mesma velocidade, sendo garantido o livre acesso a todo tipo de conteúdo, permitindo condições de igualdade a todos quanto ao acesso de informações.

Na legislação também é disciplinada a forma de utilização da Internet, trazendo como objetivos o direito a acesso à rede para todos (princípio da universalidade), o acesso à informação, ao conhecimento, o incentivo ao desenvolvimento de outros meios tecnológicos que colaboram para o acesso e a utilização do ambiente virtual.

Além disso são assegurados os registros de acessos, preservando a intimidade dos usuários. No entanto, mediante ordem judicial, o provedor responsável por manter os registros fica obrigado ao fornecimento quando tal medida puder formar conjunto probatório em processo cível ou penal.

3. CONCEITO DE CIBERCRIME

Conhecido popularmente por crimes digitais, crimes on-line, crimes eletrônicos, crimes virtuais, crimes cibernéticos, entre demais denominações, o termo cibercrime surgiu no final dos anos 90, na reunião do subgrupo do G-8 realizada em Lyon, na França, que discutiu maneiras de combate das práticas delituosas digitais por conta da grande expansão da Internet já vivenciada aquela época.

Cibercrime é compreendido como a prática de uma conduta ilícita manifestada por meio eletrônico, em que se é utilizado o recurso de Internet como meio para prática

delituosa, assim como no envolvimento de arquivos e/ou sistemas digitais. Podem ser cometidos somente em ambiente tecnológico, ocorridos, por exemplo, na manipulação de caixas eletrônicos, ou até mesmo nos crimes convencionais executados na forma digital ou que incluam alguma ação tecnológica para praticar o crime, tendo os crimes contra a honra como exemplificação.

Nesses tipos de crimes depara-se com uma grande dificuldade de provar a autoria e materialidade e até mesmo de como se provar o delito, o que dificulta bastante a investigação por parte da Polícia Judiciária junto com o Poder Judiciário, dado a facilidade encontrada por qualquer pessoa para realizar o crime de qualquer lugar do mundo, estando em um lugar completamente distante ao da vítima. Assim compreende Luiz Augusto Filizzola D'Urso:

> Com esta migração e ampliação gigantesca do universo virtual e a transferência de quase tudo para a rede, devido à informatização, os criminosos também são atraídos para este ambiente, o que resulta numa migração dos crimes para a Internet. Tal fato ocorre, pois os delinquentes notaram um novo mundo – no qual são realizadas as movimentações bancárias on-line, as compras virtuais, a comunicação digital, o trabalho à distância (Home office), dentre outras coisas –, para o cometimento de delitos virtuais (D'URSO, 2019).

Ainda existe a possibilidade do criminoso dominar diversas ferramentas tecnológicas e assim tornar mais difícil sua identificação, até por conta da escassez de policiais preparados para o combate a esse tipo de delito.

Por conta das mais variadas formas de delitos informáticos, existe a classificação predominante que separa os crimes em puros, mistos e comuns.

Os crimes cibernéticos puros são definidos como as condutas ilícitas que tem como alvo o próprio sistema de computador, ou seja, o delito na prática visa atingir o computador, seus equipamentos físicos e também seus dados e sistemas. O exemplo principal é o do agente que tem amplo conhecimento em informática e utiliza isso como meio para invadir computadores alheios.

Nos crimes mistos o uso da Internet ou sistemas informáticos são indispensáveis, sendo condição para a realização da conduta ilícita, mesmo que o bem jurídico almejado não seja informático, mas este seria instrumento essencial para a consumação da prática delituosa.

Já nos crimes cibernéticos comuns a Internet é utilizada como instrumento para o cometimento de um crime já existente e tipificado no ordenamento jurídico, sendo o meio informático mais uma forma para execução de uma conduta criminosa.

4. CRIMES INFORMÁTICOS MAIS PRATICADOS

Os recursos tecnológicos são ferramentas extremamente úteis para os seres humanos, mas também podem fazer com que pessoas sofram um revés, ou seja, possam ser vítimas de um cibercrime. Mesmo que não pareça, os crimes cometidos por meios eletrônicos são praticados frequentemente. Para ajudar na proteção contra os crimes virtuais é importante saber quais são os crimes existentes. Para isso será explanado os cibercrimes comumente praticados para que se possa adotar as condutas preventivas.

4.1 Abuso Sexual

A nomenclatura Abuso Sexual é referida para destacar os crimes de violação sexual. Abrange diversas formas de agressões sexuais, tais como o estupro, estupro de vulnerável, assédio sexual, importunação sexual, entre outros tipificados no ordenamento jurídico brasileiro.

Junto com o crescente uso da Internet, os abusos sexuais passaram a ser praticados em diversos tipos de plataformas, principalmente em redes sociais, gerando um certo conforto ao criminoso por conta da dificuldade de identificação, junto com o sentimento de impunidade. Cada caso é um caso, no entanto, na maioria das vezes o criminoso cria um perfil falso em redes sociais para se aproximar da vítima, conseguindo manter uma relação de amizade. Após ganhar a confiança da vítima, que se inicia através de uma primeira conversa, seguida para ligações de vídeos, o abusador consegue marcar encontros no intuito de praticar os abusos.

Nos mesmos moldes encontra-se a prática delituosa denominada *"grooming*". Esse nome é dado para definir o aliciamento de menores pela Internet. A intenção é alcançar a satisfação de vontades sexuais ao conseguir fotos, vídeos, mas também o contato físico com a vítima. Geralmente, é ocorrida por redes sociais.

4.2 Pornografia Infantil

Pornografia infantil é o nome dado a todos tipos de envolvimento com crianças ou adolescentes em atividades sexuais explícitas ou a representação de seus órgãos sexuais com o intuito exclusivamente sexual.

A nova redação que entrou em vigor (Lei nº 11.829, de 25/11/2008), alterando o Estatuto da Criança e do Adolescente, tipificou as condutas relacionadas à pedofilia pela Internet. Agora diversas ações que tenham relação com a divulgação, produção, consumo, venda, exposição à venda, armazenamento, transmissão, participação, aquisição de pornografia infantil são apenadas pelo Código.

O recurso digital vem sendo a cada dia mais empregado por pedófilos, por ser uma via privilegiada. Diversas são as formas de abordagem realizadas por eles. Entre as mais utilizadas estão os programas de mensagens instantâneas, salas de bate-papo (chat), blogs, e-mails e redes sociais.

Assim como na prática de abusos sexuais, o pedófilo utiliza-se da abordagem virtual, em sua grande maioria usando um perfil falso. O objetivo inicial é conquistar um vínculo de amizade com a vítima, na intenção de adquirir uma certa confiança. Estabelecida a amizade, o criminoso passa a enviar fotos e vídeos de cunho sexual, solicitando também o envio da vítima.

4.3 Registro não autorizado da intimidade sexual

No rol dos mais novos crimes cuidados pelo Código Penal Brasileiro, existe o registro não autorizado da intimidade sexual, que foi incluído pela Lei 13.772, de 19 de dezembro de 2018. Busca-se coibir a exposição não autorizada da intimidade sexual. Apesar de a lei ser bastante recente, a divulgação de intimidade perdura a tempos. Pune o criminoso que produz, registra, filma e fotografa cenas de nudez, de ato sexual ou libidinoso de outrem, bem como quem realiza montagem em fotografias alheias com intuito de colocá-las em cenas de práticas sexuais.

Conduta comumente chamada de “vingança pornográfica”, foi inspirada no caso Rose Leonel, paranaense vítima de exposição de suas fotos íntimas pelo seu ex-noivo.

4.4 Invasão de Privacidade

Um dos crimes mais comuns praticados nos dias atuais é a invasão de privacidade. O compartilhamento exacerbado de informações nas redes sociais fez com que essa prática avançasse.

Existem diversas maneiras de invadir a privacidade alheia. Uma das formas mais atuais é a invasão cibernética, que consiste na exposição da vida pessoal de outrem sem a sua autorização, disseminadas através de meios informáticos. Os principais exemplos são os compartilhamentos de fotos e vídeos, invasão de contas bancárias de terceiros, entre outras situações.

A Lei 12.737, de 30 de novembro de 2012, incluiu a "invasão de dispositivo informático" no rol de crimes do Código Penal Brasileiro. Esta Lei recebeu a alcunha de Lei "Carolina Dieckmann", por conta da atriz ter tido seu computador pessoal invadido por criminosos. Na ocasião seus arquivos pessoais foram furtados, inclusive fotos nuas que foram divulgadas na Internet. Carolina alegou ter sofrido ameaças de extorsão a pagamento em dinheiro para não ter as suas fotos divulgadas na rede.

A Lei determina a punição do delinquente que invade dispositivo móvel alheio para instalar vulnerabilidades ou obter, adulterar ou destruir informações na intenção de obter vantagem ilícita.

4.4.1 Phishing

Entre os diversos tipos de malwares (softwares malígnos desenvolvidos para acessar de forma oculta um dispositivo sem a autorização do usuário) existentes, os Phishings tornaram-se um dos golpes mais corriqueiros utilizados ultimamente. Consiste em uma maneira desonesta praticada por cibercriminosos para enganar as vítimas e fazê-las fornecer, ingenuamente, seus dados pessoais, tais como número de CPF (cadastro de pessoa física), senhas de cartões bancários, senhas de e-mails, bem como fotos pessoais. O fraudador emprega diversas formas fraudulentas para adquirir ilicitamente informações alheias. Entre as diversas formas, a mais conhecida está no envio de e-mails ou mensagens falsas, mas que em sua aparência parecem ser reais. A vítima não percebe se tratar de um golpe e clica nos links fraudulentos que levam a sites falsos.

4.5 Racismo e Injúria Racial

Historicamente a população negra foi tratada com inferioridade. Vários momentos importantes aconteceram no decorrer de épocas na luta contra o racismo, tais como o fim do Apartheid (política racial implantada na África do Sul); Elizabeth Eckford, a primeira mulher negra que estudou em uma escola para brancos nos EUA, ocorrido em meados da década de 1950 e 1960; morte de Martin Luther King, apontado como um dos maiores personagens no combate ao racismo mundial. Sua morte ocasionou diversas ações para combater o racismo.

Apesar desses grandes movimentos ocorridos mundialmente, a segregação racial e o preconceito ainda perduram. A quantidade de pessoas que cometem crimes de ódio em desfavor da população negra cresce gradualmente.

Com a facilidade oferecida pela Internet e seus meios, esses crimes foram rapidamente difundidos. Assim como já apresentado em outros crimes, os criminosos se prevalecem da dificuldade de sua identificação, utilizando perfis falsos. Também se sentem seguros por estarem por detrás de recursos tecnológicos. A sensação de anonimato causa uma falsa impressão de estar protegido e encoraja o cometimento do delito.

A Injúria Racial é tipificada do Código Penal Brasileiro. Já o crime de Racismo encontra-se na Lei 7.716, de 05 de janeiro de 1989. As duas condutas se divergem, pois na injúria racial a ofensa é cometida a uma pessoa determinada, agredindo a honra subjetiva e no racismo a afronta é feita a um grupo social, acometendo a dignidade humana.

4.6 Crimes contra honra

Inserido no Capítulo V do Código Penal Brasileiro os crimes contra a honra ocorrem quando uma pessoa ofende a imagem ou estima da outra. A ofensa pode advir através de duas vertentes: a honra subjetiva e a honra objetiva. A subjetiva é definida naquilo que a pessoa acha de si mesma, a sua autoestima. A objetiva é definida na imagem social vista pela coletividade perante a uma pessoa.

O Código Penal contempla três tipos de crimes que ofendem a honra: calúnia, difamação e injúria.

A Calúnia é tipificada no artigo 138 e pune a pessoa que, falsamente, atribui a alguém fato definido como crime. Alcança a honra objetiva da vítima. É indispensável que a pessoa que cometeu a ofensa tenha conhecimento da imputação falsa. Assim compreende Fernando Capez:

> [...] significa imputar falsamente fato definido como crime. O agente atribui a alguém a responsabilidade pela prática de um crime que não ocorreu ou que não foi por ele cometido. Trata-se de crime de ação livre, que pode ser praticado mediante o emprego de mímica, palavras (escrita ou oral). (CAPEZ, 2012, p. 283)

Já a Difamação está prevista no artigo 139 e ocorre quando alguém atribui a outro fato não criminoso, no entanto, ofensivo a sua reputação, na intenção de denegrir a imagem da outra pessoa. Assim como no crime de calúnia, a difamação atinge a honra objetiva da vítima. Fernando Capez entende:

> [...] consiste em imputar a alguém fato ofensivo à reputação. Imputar consiste em atribuir o fato ao ofendido. A reputação concerne à opinião de terceiros no tocante aos atributos físicos, intelectuais, morais de alguém. É o respeito que o indivíduo goza no meio social. A calúnia e a difamação ofendem a honra objetiva, pois atingem o valor social do indivíduo. Trata-se de crime de ação livre, que pode ser praticado mediante o emprego de mímica, palavras (escrita ou oral). (CAPEZ, 2012, p. 300)

A terceira e última modalidade de delito contra a honra é a Injúria. Prevista no artigo 140, ocorre quando alguém ofende a dignidade da outra, atribuindo-lhe qualidades negativas. Neste tipo o código protege a honra subjetiva da vítima. No mesmo sentido explana Fernando Capez:

> A injúria, ao contrário da difamação, não se consubstancia na imputação de fato concreto, determinado, mas, sim, na atribuição de qualidades negativas ou de defeitos. Consiste ela em uma opinião pessoal do agente sobre o sujeito passivo, desacompanhada de qualquer dado concreto. São os insultos, xingamentos (p. ex., ladrão, vagabundo, corcunda, estúpido, grosseiro, incompetente, caloteiro etc.). (CAPEZ, 2012, p. 307)

Nos dias atuais, com os recursos tecnológicos fazendo parte essencial da vida humana, sem sombras de dúvidas os crimes de calúnia, injúria e difamação expandiram-se.

Não é por conta das ofensas terem sido cometidas na Internet é que elas são impunes. No estado de Santa Catarina, uma loja de materiais esportivos foi condenada ao pagamento de treze mil reais para uma funcionária que, constantemente, era xingada por seu chefe e as mensagens eram compartilhadas no aplicativo WhatsApp. Outro caso aconteceu no Rio Grande do Sul, em que a amante foi condenada a pagar dois mil reais a esposa do marido por chamá-la de "coitada, otária, chifruda, burrinha". Em mais um caso, uma jovem de vinte e um anos foi ridicularizada em um grupo de WhatsApp, composto por dezessete amigos. Um dos membros relatou por meio de áudio ter mantido relações sexuais com a jovem e ter sido o responsável por ela ter perdido a virgindade. Foi determinado o pagamento de indenização de dez mil reais por difamação e danos morais.

Assim como nos demais crimes, é cada vez mais corriqueiro o acontecimento de delitos contra a honra cometidos na Internet, principalmente em redes sociais e no aplicativo WhatsApp.

5. COMO AGEM OS CIBERCRIMINOSOS

A evolução da tecnologia junto com o crescente desenvolvimento de aplicativos e a facilidade de conexão com a Internet, facilitou para que criminosos olhassem nisso um novo meio de atuação maliciosa, a fim de obterem maior aproximação das vítimas para o cometimento de seus crimes.

Existem diferentes formas utilizadas pelos criminosos para a prática de um crime virtual, sendo a maioria baseada na vulnerabilidade de aparelhos. Para vulnerabilidade André Campos entende:

> Vulnerabilidade são fraquezas presentes nos ativos de informação, que podem causar, intencionalmente ou não, a quebra de um ou mais dos três princípios de segurança da informação: confidencialidade, integridade e disponibilidade. (CAMPOS, 2006, p. 11)

O auxílio de recursos informáticos faz transparecer o anonimato para o delinquente, principalmente quando se trata de um perfil falso, dando-lhes uma falsa impressão de proteção, relacionada ao pensamento de que a punição é improvável. Essa prática pode ser muito bem vista quando tratamos de um crime de abuso sexual e quando se deseja a divulgação não permitida de imagens íntimas. O criminoso aproxima-se da

vítima como se fosse um amigo, levando-a a sensação de confiança. Depois de adquirido um vínculo, ocasião em que a vítima já se encontra confortável com a presença virtual do criminoso, este então passa a enviar mensagens de conteúdos eróticos, alegando ser ele. Também passa a pedir fotos íntimas das vítimas para ganhar mais confiabilidade. No fim, consegue marcar encontros pessoais ou mesmo não marcando, já tem em mãos conteúdos pornográficos disponibilizados pelas próprias vítimas. Essa prática é muito comum também no crime de pornografia infantil.

As redes sociais são as principais fontes de informações para a colheita de elementos por parte dos criminosos. Por meio delas as vítimas passam a ser presas fáceis, pois informam a maioria de seus dados pessoais.

Pedro Monteiro Eleutério e Mateus Polastro argumentam que:

> [...]. Utilizando perfis falsos, os abusadores tentam se aproximar das vítimas por esses meios, sendo que as redes sociais acabam trazendo mais uma grande vantagem ao abusador: o fato do perfil das vítimas conter informações preciosas sobre suas preferencias pessoas, como filmes, comidas e passeios favoritos. Os abusadores utilizam essas informações para se aproximarem das vítimas fingindo possuir gostos em comum (ELEUTÉRIO, POLASTRO, 2016, p. 250).

As redes sociais são bastantes vulneráveis, por conta de ser facilitado o cadastro de perfil, promovendo a criação de diversos perfis falsos (*fakes*) na intenção de enganar as vítimas.

Não bastando isso, nas próprias redes sociais existem pessoas que cometem crimes racistas. O avanço tecnológico e a facilidade da Internet também facilitaram para que o racismo fosse disseminado com mais facilidade. Pessoas com más intenções aproveitam da dificuldade que é para identificar o responsável pela postagem, e promovem o ódio com comentários preconceituosos. Nesse sentido explana Ilton César Martins:

> Todos sabemos que não é de hoje que as redes sociais têm servido de palanque para que pessoas vomitem preconceito e ódio. Igualmente sabemos que as denúncias e punições, no entanto, não parecem fazer frear a necessidade de muitos usuários das redes sociais de exporem os seus preconceitos [...] O que antes era dito dentro de um círculo pessoal, ou entre familiares, agora é colocado na rede sem qualquer constrangimento, como se não fugisse da normalidade. Ou seja, nos últimos anos a internet tem constituído um espaço privilegiado para a prática de crimes de ódio, em especial o racismo (MARTINS, 2014).

Também com o auxílio da Internet os criminosos invadem a privacidade das vítimas, com a prática de crimes, no intuito, de obter informações pessoais e confidenciais delas. Esse comportamento desonesto normalmente é realizado através de criação de sites falsos que imitam o verdadeiro, geralmente com o envio de e-mails falsos ou no direcionamento para os sites falsos. Como já estudado, essa prática é chamada de *Phishing*. Com ela a vítima fornece dados como senhas de cartão bancário, endereço, CPF, entre outros, acreditando na confiabilidade de sites ou e-mails. Conduta parecida é cometida com desenvolvimento de um programa malicioso, conhecidos por *Malware*, destinado a infiltrar no computador pessoal da vítima, passando a monitorar o que é feito, ou até mesmo causar danos irreparáveis, além da coleta de informações íntimas e pessoais da vítima.

6. COMO AGIR DIANTE DE UM CRIME VIRTUAL

Seja qual for o cibercrime é imprescindível que as pessoas saibam como proceder quando forem vítimas.

No primeiro momento é importante identificar qual a modalidade de crime ocorreu. Como já estudado, várias são as formas delituosas cometidas por meios eletrônicos.

Se for o caso, deverá notificar o provedor responsável pela rede social ou site em que se encontra a conduta delitiva. Assim, a empresa encarregada ficará obrigada a retirar a ofensa e/ou obter os dados da ação do criminoso, identificando o número de IP (Protocolo de Internet) utilizado, a fim de identificá-lo.

Na grande maioria dos crimes é indispensável ser preservadas todas as provas. Conteúdos como conversas mantidas em aplicativos de comunicação, mensagens de correio eletrônico, conteúdos de páginas, especialmente em redes sociais, devem ser preservados. É recomendável que imprima ou salve em mídia toda coleta de evidências do crime virtual praticado. É necessário dirigir a Delegacia de Polícia para formalização de um boletim de ocorrência.

Após o registro, a Polícia Civil aplicará todos os recursos de Polícia Judiciária viáveis ao caso.

Em determinadas situações é indicado procurar auxílio de um advogado, pois muitos dos delitos eletrônicos causam danos plausíveis de solicitação de indenização.

7. SEGURANÇA DA INFORMAÇÃO E CONDUTAS DE PREVENÇÃO

Tamanha é a disseminação de informações que ocorrem na Internet, e por isso muitos crimes novos surgiram e outros tornaram-se mais fáceis de serem praticados. Muitos estudos foram e continuam sendo feitos para aprimorar as formas de segurança da informação, com a finalidade de evitar riscos de danos e assegurar a privacidade das pessoas.

A segurança da informação relaciona-se diretamente com a forma de proteção de dados e informações de uma pessoa ou até mesmo de uma empresa, com a finalidade de garantir o tráfego seguro das informações, evitando, assim, o acesso de pessoas, softwares e dados indesejáveis. Desse modo explanam os autores:

> A segurança da informação trata da proteção dos sistemas de informação e do acesso, utilização, divulgação, interrupção, modificação ou destruição não autorizados à informação, preservando a confidencialidade, integridade / autenticidade e disponibilidade de informações. O objetivo é mitigar riscos e proteger a informação das ameaças que têm impacto negativo sobre a continuidade do negócio e, em última instância maximizar o retorno sobre investimentos e oportunidades de negócios (SOUZA et al, 2016, p. 241).

Uma das principais formas de manter a segurança e criar restrições de acessos indesejáveis é a utilização de um dos dispositivos mais importantes dos sistemas de tecnologia: o Firewall.

O Firewall é um dispositivo de segurança que tem objetivo monitorar a entrada e saída de informações. Nesta checagem o dispositivo bloqueia o tráfego de informações consideradas invasivas, ajudando a impedir o acesso de vírus, malwares, crackers. Portanto, para manter a eficácia no bloqueio dos dados indesejáveis, é imprescindível conservar o firewall devidamente configurado e atualizado. No entendimento de Gabriella D. de Oliveira, Rafaela K. Galdêncio de Moura e Francisco de A. Noberto Galdino de Araújo:

> Um sistema de segurança seguro dentro de uma organização é o software firewall, pois ele possibilita um ambiente seguro com outros softwares que fazem criptografia. Estes mecanismos de criptografia permitem a transformação reversível da informação de forma a torná-la identificáveis a terceiros. Utiliza-se para tal, algoritmos determinados e uma chave secreta

> para, a partir de um conjunto de dados não criptografados, produzir uma sequência de dados criptografados (OLIVEIRA, MOURA, ARAÚJO, 2012, p. 8).

O antivírus é outro recurso visto como essencial e que compõe a linha de frente no cuidado da vulnerabilidade, prevenção e segurança da informação. Diante das ameaças virtuais, a instalação de um antivírus passou a ser indispensável. Dentre os benefícios da instalação do programa, é possível relacionar a maior agilidade em detectar o vírus; controle de sites suspeitos; aviso do uso de dispositivos móveis, tais como *pen drive*, que pode estar contaminado; maior proteção dos aparelhos eletrônicos; proteção contínua, entre outras. Por isso é primordial ter instalado um antivírus no aparelho, bem como mantê-lo atualizado.

Algumas condutas de prevenção de riscos devem ser tomadas pela própria pessoa pra que não deixe o aparelho vulnerável. Precisa-se de ter cuidado e muita atenção para garantir a segurança das informações. Existem algumas dicas de segurança importantes de serem aplicadas e que evitam quase que por completa a chance de tornar-se vítima de um cibercrime: sempre utilize senha; mantenha aplicativos atualizados; tenha sempre autenticação; procure não abrir mensagens de remetentes não conhecidos; procure controlar o acesso à rede; não se deve abrir *links* que não sejam identificados ou ainda visitar sites desconhecidos; sempre ter atenção em quem está em volta no momento em que for digitar senhas ou acessar conteúdo confidencial; entre outras.

8. CONCLUSÃO

Este artigo procurou analisar, dentro das possibilidades, a evolução dos crimes que são cometidos com o auxílio de recursos tecnológicos diante do crescimento da tecnologia e de seus recursos, discorrendo sobre as causas e efeitos dos crimes eletrônicos mais praticados, bem como as principais ações dos cibercriminosos e suas especificações.

A Internet, que de certa forma deveria apenas ser aproveitada com recursos benéficos, infelizmente passou a ser utilizada para ações criminosas, o que vem crescendo constantemente. Os cibercrimes auferiram lugar de destaque na Internet com o avanço das tecnologias, até por conta da facilidade em cometer crimes e da dificuldade no esclarecimento da autoria.

Os crimes apresentados são apenas alguns diante dos vastos existentes. Em face da extensa circulação de informações que ocorrem na Internet, com uma grande maioria desses dados serem relacionados a informações pessoais de usuários, fez com que criminosos encontrassem maior facilidade para suas ações maliciosos. Surgiu-se a segurança da informação. No presente artigo pode analisar as formas de segurança e medidas de prevenção para o combate das ações delituosas.

Embora seja considerado difícil o combate aos cibercrimes, é muito relevante que as vítimas tomem ciência de como recorrerem diante de um crime virtual. Apesar da existência de trabalho policial específico, as técnicas utilizadas pelos cibercriminosos vêm em constante evolução, por isso a coleta das informações realizadas pela vítima é imprescindível.

Portanto, a observância dos modelos básicos de prevenção deve ser adotada por cada usuário, a fim de evitar grande chance de ser vítima de um cibercrime.

REFERÊNCIAS

BITENCOURT, Jesiel. **Gestão da segurança da informação**: desafios e perspectivas. 2018. 72 f. Trabalho de Conclusão de Curso - Universidade Federal de Santa Catarina Campus Araranguá, Santa Catarina, 2018.

CAMPOS, André L. N. **Sistema de Segurança da Informação**: Controlando os Riscos. Florianópolis: Visual Books, 2006.

CAPEZ, Fernando. **Curso de Direito Penal**: Parte Especial 2. 12. ed. São Paulo: Editora Saraiva, 2012, p. 283-307.

CASTRO, Luiz. **Legislação atual não contempla a moderna invasão de privacidade**. 2017. Disponível em: https://www.conjur.com.br/2017-jun-30/luiz-castro-leis-nao-contemplam-moderna-invasao-privacidade. Acesso em: 11 ago. 2019.

CORDEIRO, Ana Dias. **Abusos sexuais que começam por conversas na Internet**. 2017. Disponível em: https://www.publico.pt/2017/06/04/sociedade/noticia/abusos-sexuais-que-comecam-por-conversas-na-internet-1773949. Acesso em: 11 ago. 2019.

D'URSO, Luiz Augusto Filizzola. **Tudo sobre os cibercrimes**. 2019. Disponível em: https://politica.estadao.com.br/blogs/fausto-macedo/tudo-sobre-os-cibercrimes/. Acesso em: 08 ago. 2019.

FILHO, Jair Lúcio Alves; MARQUES, Bruna Moraes. **Breve análise dos princípios e garantias do marco civil da internet**. Anais do Encontro Virtual de Documentação em Software Livre e Congresso Internacional de Linguagem e Tecnologia Online. 2017.

Disponível em: http://www.periodicos.letras.ufmg.br/index.php/anais_linguagem_tecnologia/article/view/12156/10380. Acesso em: 14 nov. 2019.

FIRMINO, César Augusto Castor. **Preconceito nas redes sociais**: impunidade e anonimato favorecendo a propagação dos crimes de ódio contra os negros. 2018. 24 f. Trabalho de Conclusão de Curso – Centro Universitário Tabosa de Almeida – Asces Unita, Caruaru, 2018.

MARINHO, Marcos de Andrade Sousa. **Pornografia infanto juvenil e invasão há rede de computadores**. 2018. 20 f. Trabalho de Conclusão de Curso – Instituto de Pós-Graduação - IPOG, Brasília, Distrito Federal, 2018.

MARTINS, Ilton Cesar. **Tudo sobre os cibercrimes**. 2019. Disponível em: https://politica.estadao.com.br/blogs/fausto-macedo/tudo-sobre-os-cibercrimes/. Acesso em: 08 ago. 2019.

OLIVEIRA, Gabriella Domingos de; MOURA, Rafaela Caroline Gaudêncio de; ARAÚJO, Francisco de Assis Norberto Galdino de. **Gestão da segurança da informação**: perspectivas baseadas na tecnologia da informação. 2012. Disponível em: http://portaldeperiodicos.eci.ufmg.br/index.php/moci/article/viewFile/2111/1311. Acesso em: 10 ago. 2019.

PIZARRO, Ludmila. **Crimes cibernéticos atingem 62 milhões no Brasil em 2017**. 2018. Disponível em: https://www.otempo.com.br/capa/economia/crimes-ciberneticos-atingem-62-milhoes-no-brasil-em-2017-1.1572879. Acesso em: 19 mar. 2019.

POLASTRO, Mateus; ELEUTÉRIO, Pedro Monteiro. **Tratado de Computação Forense**: Capítulo 7 – Exames Relacionados à Pornografia Infanto-Juvenil. Millennium Editora, 2016.

SOUZA, Jackson Gomes Soares, *et al*. **Gestão de riscos de segurança da informação numa instituição pública federal**: um estudo de caso. Revista Eniac Pesquisa, Faculdade ENIAC, v. 5, n. 2, p. 240–256, 2016.