KARLA LORRANY DA SILVA DUARTE

CRIMES CIBERNÉTICOS E OS IMPACTOS DA LEI GERAL DE PROTEÇÃO DE DADOS

CURSO DE DIREITO- UniEVANGÉLICA

2022

KARLA LORRANY DA SILVA DUARTE

CRIMES CIBERNÉTICOS E OS IMPACTOS DA LEI GERAL DE PROTEÇÃO DE DADOS

Monografia apresentada ao Núcleo de Trabalho Cientifico do curso de Direito da UniEvangélica, como exigência parcial para a obtenção de grau de bacharel em Direito, sob orientação do professor Me. Adriano Gouveia Lima.

ANÁPOLIS-2022

KARLA LORRANY DA SILVA DUARTE

CRIMES CIBERNÉTICOS E OS IMPACTOS DA LEI GERAL DE PROTEÇÃO DE DADOS

Anápolis 28 de novembro de 2022.

BANCA EXAMINADORA

_____

_____

RESUMO

A presente pesquisa analisa os crimes cibernéticos previstos na legislação brasileira e abordar sobre os impactos que a Lei Geral de Proteção de Dados pode causar nesse tipo de delito. O objeto desta pesquisa em síntese, foi a lei 13.709/2018 que dispõe sobre a Lei Geral de Proteção de Dados, a Lei 14.155/2021 que modificou e incluiu alguns dispositivos do Código Penal e do Código de Processo Penal, promovendo alterações referentes aos crimes de invasão de dispositivos informáticos, furto mediante fraude eletrônica, estelionato mediante fraude eletrônica, dentre outras. Com o estudo analítico proposto, foi utilizada pesquisas bibliográficas, servido de estante às consultas doutrinas e artigos científicos.

Palavras-chave: Crimes Cibernéticos. LGPD. Internet. Mundo Digital. Evolução.

SUMÁRIO

INTRODUÇÃO

O presente trabalho monográfico, no primeiro capítulo tem como objetivo imprescindível, analisar acerca dos crimes cibernéticos, abordando a sua tipificação em sentido lato sensu, o seu conceito, as suas espécies, suas características, apresentando o marco civil da internet, estudar os aspectos trazidos pela Constituição Federal acerca desse crime.

No segundo capitulo, será abordado acerca dos crimes cibernéticos em espécie contidos no Código Penal, mencionando quem são os sujeitos desse delito e por fim deste capitulo será feito uma análise de crimes cibernéticos.

E por fim, no último capítulo será mencionado sobre a conexão dos Crimes Cibernéticos com a Lei 11.709/2018 que dispõe sobre a Lei Geral de Proteção de Dados, abordando quais são os impactos que esta lei pode trazer para esse tipo de crime, o que pode ser feito para maior proteção dos dados tratados por redes de computadores e dispositivos eletrônicos, sejam eles pessoais ou empresariais, a importância que a LGPD tem sobre esse crime, e como a sociedade pode se resguardar para não se tornar vulnerável perante os criminosos digitais.

CAPÍTULO I – OS CRIMES CIBERNÉTICOS

Esse capítulo aborda sobre o histórico e evolução da internet mencionando quando a questão criminal ingressou no mundo digital, será apontado quem são os usuários potencialmente criminosos na Web, e quais são as condutas por eles praticadas, que os levam de um simples usuário a um criminoso digital.

A mundialização e a difusão da Web e dos dispositivos eletrônicos, como computadores, smartphones, foi algo revolucionário para a sociedade, isso não é de se negar, mas ao mesmo tempo que facilita a comunicação instantânea entre milhares de pessoas, proporcionando formas de negociação, vem acontecendo muitas condutas ilícitas não aprovadas pelo nosso ordenamento jurídico.

E para finalizar esse capítulo, será abordado sobre o ambiente criminal cibernético, desde a otimização da internet como meio de comunicação/negociação até ao surgimento de condutas criminosas no meio virtual.

1.1 – Histórico sobre a internet e a questão criminal

A internet é um sistema de redes de computadores interconectados de proporções mundiais, atingindo mais de 150 países e reunindo cerca de 300 milhões de computadores. E teve sua origem em meados dos anos 60, especificamente em 1963, em meio a um cenário de Guerras, sendo elas, Guerras Espaciais e a Guerra Fria (DIZARD, 2000).

Na época era indispensável o compartilhamento de informações entre localizações distintas, e com isso surge a internet como uma ferramenta de comunicação alternativa entre os militares (DIZARD, 2000).

Uma equipe de programadores e engenheiros eletrônicos, contratados pelo Departamento de Defesa dos Estados Unidos, desenvolveu o conceito de uma rede sem nenhum controle central, por onde as mensagens passariam divididas em pequenas partes em uma rede onde cada computador seria apenas um ponto, e se caso ficasse inviável de operar, não aconteceria a interrupção da rede. Desta forma, as informações seriam transmitidas com rapidez e flexibilidade (DIZARD, 2000).

E se tratando do assunto, Marcelo Sávio de Carvalho (2006, p. 28) Mestre das Ciências em sua dissertação de mestrado, menciona que:

> A tensão da Guerra Fria entre Estados Unidos e União Soviética tiveram grande influência na caracterização e desenvolvimento no advento da criação da internet, uma vez que, serviu de estímulo para a melhorar o sistema, e transformar ele ainda mais inovador e mais propício a novos usuários.

Depois da criação da internet, que iniciou as atividades com base na necessidade dos militares de se comunicarem de forma mais ágil, a rede de internet começa a surgi nas Universidades (PAESANI, 2000).

Em outubro de 1969, com uma comunicação entre a Universidade da Califórnia e um centro de pesquisa em Stanford, entrou em operação a ARPAnet (Advanced Research Projects Agency Network), onde inicialmente interligou quatro computadores. Rapidamente, mais computadores pertencentes a outras universidades se interligaram (PAESANI, 2000).

A ARPANET que foi uma proposta criada pela Agência de Projetos de Pesquisa Avançada dos Estados Unidos, foi o marco pioneiro para evolução da internet, pois foi a primeira rede operacional de computadores interativa à base de computação de dados (PAESANI, 2000).

Com o final da guerra entre EUA e URSS, houve a abertura da rede para interesses comerciais, quando os Estados Unidos começaram a “comercializar” a internet. Em seguida, deu-se início a uma revolução tecnológica, que impactou toda a infraestrutura da internet, deixando de ser apenas um sistema de acesso restrito às minorias, para se tornar o meio de comunicação mais utilizado no mundo (PAESANI, 2000).

A Internet chegou ao Brasil em setembro de 1988 quando o laboratório Nacional de Computação Científica (LNCC) no Rio de Janeiro acessou o Bitnet através de uma conexão de 9600 bits/s juntamente com a Universidade de Maryland (GUIZZO, 1999).

No final de 1994, o governo brasileiro, que até então pouco fizera com a internet no Brasil, anunciou, por meio do Ministério da ciência e Tecnologia e do Ministério das comunicações sua intenção de investir em novas tecnologias (GUIZZO, 1999).

Com o tal pronunciamento do governo brasileiro, houve a criação da estrutura necessária para a exploração comercial da internet no Brasil, e tudo foi responsabilidade da Embratel e da RNP. Após a Embratel lançar de forma experimental o serviço de acesso à internet, o Ministério das comunicações tornou pública a posição do governo brasileiro de que não haveria monopólio e que o mercado de serviços de Internet no Brasil seria o mais aberto possível (GUIZZO, 1999).

Desde então, a internet começou a obter uma apreciação mais próxima da que temos atualmente, o que nos leva a ter uma definição de crimes cibernéticos mais notáveis. Com a constante evolução da internet, do mundo virtual, o cibercrime deu início a uma nova fase, desde quando a criptografia se tornou muito utilizada para auxiliar dados digitais do universo corporativo, tornando assim objeto de reverência dos criminosos digitais (PAESANI, 2000).

A internet é usada para várias finalidades, seja para trabalho, estudo ou entretenimento, o que não se pode negar e que a internet se tornou uma essencialidade na vida das pessoas. E há várias maneiras de acessar os meios digitais nos dias de hoje, seja através de notebooks, tablets ou smartphones, e com isso, consequentemente tem-se diversas formas de invadir os dispositivos.

Como o que foi mencionado sobre o histórico da internet, o autor Fabrizio Rosa traz um conceito de crimes na internet, vejamos:

> A conduta atente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento dedados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar; 2. O 'Crime de Informática' é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão; 3. Assim, o 'Crime de Informática' pressupõe elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador, utilizando-se software e hardware, para perpetrá-los; 4. A expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável, contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão; 5. Nos crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, [entre outros] (ROSA, 2002).

Com o que foi exposto acima, conclui-se que, mesmo sabendo que a internet se tornou algo valoroso na vida de milhares de pessoas, não se pode negar que a internet não trouxe apenas benefícios a seus usuários, mas também trouxe consigo, as possibilidades de suceder comportamentos criminosos no mundo digital.

1.2 – Usuários potencialmente criminosos na Web

Em tempos atuais, a internet é o maior sistema de comunicação do mundo, com mais armazenamento de dados, e com os mais variados meios que visam facilitar a vida do usuário. No mundo digital, os usuários podem navegar em diversos sites, seja para estudos, trabalhos, entretenimentos, e não se é de negar que a internet facilitou as relações comerciais no mundo (ROSSINI, 2004).

Porém, como falado anteriormente, a internet além de grandes inovações traz consigo usuários com más intenções, que usam os meios digitais para causar graves danos, seja para pessoa física ou pessoa jurídica, e é aí que entra a prática ilícita que é um crime, que atualmente é chamado de crimes cibernéticos (ROSSINI, 2004).

O autor Moisés de Oliveira Cassanti, a prática de condutas delituosas chamadas de crimes cibernéticos, pode-se averiguar a existência de dois usuários potencialmente criminosos na web, sendo eles:

> As condutas ilícitas que ocorrem na internet, geralmente estão diretamente ligadas a dois usuários o *hacker* e o *cracker*, tradução e o vocabulário "*hacker"* estão relacionado a crimes virtuais, mas os verdadeiros criminosos são os crackers. A diferença entre esses dois usuários está na maneira como fazem uso do *know-how* tecnológico, que é denominado como o conjunto de conhecimentos práticos, seja elas fórmulas secretas, técnicas tecnológicas, procedimentos (CASSANTI, 2014).

Os hackers são programadores que possuem um conhecimento vasto sobre tecnologia e internet, porém eles não usam, a princípio, seus conhecimentos para praticar condutas ilícitas (CASSANTI, 2014).

Já os crackers, no qual a palavra deriva do verbo em inglês "*to crack*", que significa quebrar, e dentro das condutas que são praticadas por eles estão a prática de quebra de sistemas de segurança, códigos de criptografia e senhas de acesso a redes, de forma ilegal e com a intenção de invadir e sabotar sistema, dispositivos eletrônicos para fins de obter vantagem ilícita (CASSANTI, 2014).

Em relação aos usuários potencialmente criminosos na internet, o doutrinador Rossini aborda:

> De acordo a Conferência das Nações Unidas sobre Comércio e Desenvolvimento o Brasil está em quarto lugar quando o assunto é quantidade de usuários conectados à internet. Com números tão exorbitantes, sabe-se o porquê de termos tantos delitos cibernéticos acontecendo a cada momento, a cada instante tem um golpe novo sendo aplicado, uma forma diferente de acessar nossos dados (ROSSINI, 2004).

Sem mencionar as altas práticas de condutas de estelionatos e das fraudes virtuais. Salienta o aumento de divulgações de fotos intimas sem o

consentimento de quem é exposto, causando transtornos que saem da esfera virtual, passando para área psicológica, e tornando os danos sofridos irreversíveis (BITTENCOURT, 2016).

Nesse contexto, destaca-se o quanto é importante ter um ordenamento jurídico firme e coeso, que tem o objetivo proteger e assegurar a os usuários, punindo com vigor invasores, além dos demais crimes ocorridos no espaço cibernético, garantindo assim a segurança, assim como nos é garantido na Carta Magda do Brasil, a Constituição Federal de 1988, faça a saber:

> Artigo 5º- Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: Inciso X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação (Brasil, 1988).

Diante do exposto, é compreensível que necessitamos que o ordenamento jurídico esteja sempre em conformidade com os avanços da era digital, trazendo verdadeiras punições para quem comete condutas delituosas no espaço digital.

1.3 – Ambiente criminal cibernético

O ambiente onde mais ocorrem os crimes cibernéticos é na internet, e atualmente como sabemos a internet deixa de ser apenas uma rede onde conectam pessoas, passando também a ser um dos ambientes mais propícios para prática de condutas ilícitas, possuindo muitas brechas e poucas leis específicas para os criminosos digitais (BARROS; GARBOSSA; CONTE, 2007).

A internet juntamente com as redes sociais tem um espaço gigantesco onde os usuários podem se comunicar com outras pessoas, fazerem negócios, expressar ideias e opiniões, tendo limites e observando os direitos das outras pessoas (BARROS; GARBOSSA; CONTE, 2007).

É claro, que nem todos usam a internet para esses fins, tornando a rede que mais conectadas pessoas no mundo em um ambiente de crimes virtuais, podendo gerar milhões reais para os criminosos, principalmente se for roubo de dados de uma empresa grande e renomada (BARROS; GARBOSSA; CONTE, 2007).

Algumas pessoas pensam que internet é terra sem lei, que não possuem regras, mas desde 2014, o espaço cibernético possui como uma das legislações o Marco Civil da internet, onde estabelece os direitos e deveres dos usuários da internet, prevê penas a quem comete condutas ilícitas dentro do ambiente digital, juntamente com o amparo do Código Penal e do Código Civil (BARROS; GARBOSSA; CONTE 2007).

Hoje, muitos crimes acontecem na internet, como a invasão de computadores, celulares, sistemas internos de empresas, seja para roubo de dados, invasão de privacidade, ataques nas redes sociais, como injúria, difamação e calúnia, dentre muitos outros.

O porquê de estar acontecendo tantos crimes cibernéticos é que os criminosos acham menos “trabalhoso” invadir um sistema interno de uma grande empresa e pedir resgate pelos seus dados podendo receber milhões de reais por isso, do que cometer um roubo a mão armada na rua.

Segundo o doutrinador Garbossa, o conceito de espaço cibernético é:

> O espaço cibernético não contém um corpo físico, por isso traz a definição de construção social do mundo real, sendo assim, é uma construção feita de imagens que se assemelham ao mundo físico. Todo esse processo deu origem ao ciberespaço (GARBOSSA, 2007).

O ambiente onde ocorrem os cibercrimes é gigantesco, e dentro dele há inúmeros outros ambientes, porém, os mais populares são a Surface Web (internet pública), a Deep Web e a Dark Web (DAOUN, 1999).

A seguir falado dos ambientes criminais cibernéticos mais populares da internet atualmente, será abordado o conceito de cada um deles, e o que esse ambiente pode englobar.

A Surface Web conhecida como internet pública é a rede que temos mais acesso atualmente, ela é de fácil acesso, pois não requisita a necessidade de softwares específicos para navegar na internet, ou seja, a Surface Web, é o local onde fazemos nossos acessos diários, onde fazemos pesquisas, acessamos redes sociais e etc (DAOUN, 1999).

A Deep Web é tradicionalmente traduzida como “internet profunda”, ela é gigante, tendo de 500 a 5.000 vezes mais conteúdo do que a Surface Web, ela é formada através de dados que não estão organizados, não podendo ser conectados por meio de uma simples busca. Desta maneira, a Deep Web se torna uma parte da internet mais “profunda”. O autor Alexandre Jean Daoun classifica em duas categorias, as maneiras como a Deep Web são profundas, sendo elas:

> A obscuridade e a autenticação, a primeira refere a inaptidão de encontrar um recurso da Web em algum mecanismo de busca, sendo que, pode ser resolvido de forma fácil incorporando um arquivo criptografado adequado a um site, impedindo os rastreadores que no método de pesquisa exibem tais resultados. Já o segundo, que é a autenticação, são métodos que estabelecem identificar uma pessoa quando ela está acessando algum sistema, pode ser por meio de um mecanismo de busca, de login, de informações, só basta que os usuários possuam credenciais autenticas (DAOUN, 1999).

A Dark Web, é mais popular que a Deep Web, ela é uma rede fechada, usada para transmitir informações de conteúdos no anonimato, só podendo ser acessado com softwares específicos ou por alguma rede segura ou criptografada. Ela também está associada com atividades ilícitas online, no qual seja venda de dados de empresas, pode se dizer que a Dark Web é onde encontram os dados advindos de atividades maliciosas, e lembrando que esse ambiente só pode ser acessado por meio de ferramentas especificas, softwares avançados (DAOUN, 1999).

Para entender de modo claro, a Deep Web é uma área da internet que guarda qualquer tipo de informação, seja elas, informações de bancos, tokens,

logins, e precisa de criptografia para ser acessada e a Dark Web é uma camada mais profunda da Deep Web, onde o seu acesso é muito mais restrito, podendo assim, ser acessada apenas com softwares específicos.

De forma resumida, para se operar na Deep Web, existe o The Onion Routee (browser) que é considerado um software, um provedor independente, afastando os plug-ins que identificam os IP's, possibilitando ao usuário ingressar na Web de forma anônima (BARROS; GARBOSSA; CONTE, 2007).

Conforme aborda os doutrinadores Marco Antônio de Barros, Daniella D'arco Garbossa e Christiany Pegogari Conte, a segmentação da internet em camadas pode ocasionar algumas confusões entre a Dark Web, Deep Web. Sendo assim, as camadas apresentam a seguinte divisão:

> A camada número 0 está relacionada a sites mais comuns como, Instagram, Google, dentre outros; a camada número 1 que está relacionada a sites isolados, como Reddit Digg, este site citado funciona como uma rede social onde usuários postam notícias, conversam de forma parecida com um fórum; a camada número 2 está relacionada a sites ocultos que não aparecem nos resultados do Google; a camada número 3 está relacionada a pornografia infantil, vírus, pirataria, ela é o começo da Deep Web; a camada número 4 está relacionada ao tráfico de animais, pornografia infantil incluindo pornografia de bebês, filmes e vídeos banidos e venda de drogas. A camada número 5 está relacionada ao tráfico de pessoas, assassinos de aluguel, sociedades secretas, seitas satânicas, vendas de armas e outros; a camada número 6 está relacionada ao campo de batalha dos hackers com muitas informações encriptadas, só decifráveis por computadores quânticos; a camada número 7 é formada por pessoas que detém poder, que lutam para chegar até a camada 8 e não querem concorrência, se tornando assim, um local cheio de vírus e códigos maliciosos, para evitar que qualquer pessoa chegue à camada 7 para evitar a concorrência; já a camada número 8 está relacionada a grupos terroristas, seitas e muitas lendas (BARROS; GARBOSSA; CONTE 2007).

Diante do que foi exposto nesse primeiro capítulo, vemos que, a constante evolução da internet ao mesmo tempo que é algo muito bom para a sociedade, também se torna algo ruim onde ocorrem os crimes cibernético, que são as atividades ilícitas praticadas na internet, por meio de dispositivo eletrônicos, como computadores e celulares, ou seja, o meio digital é o ambiente criminal onde os criminosos praticam tais condutas delituosas.

Sendo assim, o Poder Legislativo observou a necessidade de criar uma lei que fosse capaz de impor sanções para quem praticasse condutas ilícitas na internet. Atualmente temos a Lei nº 12.737/12, que é conhecida como Lei Carolina Dieckmann (BRASIL, 2012), que tem o objetivo de punir indivíduos que invadem dispositivos informáticos para fins ilícitos.

A entrada da Lei 12.737/12 (BRASIL, 2012), em vigor reproduziu mudanças significativas no ordenamento jurídico brasileiro, e que apesar de existir leis que implicam sanções para certas condutas na internet, acaba que ainda surgem brechas e lacunas no Direito, tirando a parte de que as leis são diariamente interpretadas de maneiras distintas por vários doutrinadores, juízes e etc.

É considerável ressaltar que, apesar do contexto atual ser mais tendencioso que ocorra mais crimes na internet, juntamente com as brechas contidas na legislação, se faz ainda mais necessário a conscientização da população, para que assim, evite ainda mais condutas ilícitas advindas do meio da internet.

Destarte, vários outros pontos relacionados a internet foram tratados nesse capítulo de forma objetiva, desde a evolução histórica da internet, passando por quem são os usuários potencialmente criminosos na internet, e terminando nos ambientes onde ocorrem os crimes cibernéticos.

CAPÍTULO II – CRIMES CIBERNÉTICOS

Sabe-se que crimes cibernéticos consistem em praticar condutas ilícitas através da rede de internet, por meio de computadores, dispositivos eletrônicos e entre outros e eles são classificados de acordo como esses crimes são praticados (WENDT; JORGE, 2012).

Mesmo com tanta evolução, há uma certa ausência na legislação para punir, julgar esses tipos de condutas/crimes, mas mesmo existindo essa carência na lei, cabe ao ordenamento jurídico julgar quem visa praticar essas condutas ilícitas (WENDT; JORGE, 2012).

A priori, o tema deste capítulo será descrever quais são os crimes cibernéticos dentro do Código Penal Brasileiro, mencionando também algumas legislações especificas relacionadas a este assunto.

A posteriori, estudaremos quem podem ser os sujeitos deste crime, ou seja, quem pode praticar esse tipo de crime. E por último, no último tópico faremos algumas análises de alguns crimes cibernéticos.

2.1- Os crimes cibernéticos no Código Penal

O objetivo deste tópico é abordar um rol de crimes que podem ser realizados por meio da internet, através de redes de computadores, dispositivos celulares. Sabe-se que, o Código Penal é de 1940, na época ele foi pensado em

outro paradigma, diferente do que vivemos hoje, por isso que, de lá para cá foi necessário algumas modificações, alterações, criação de algumas leis especificas para suprir lacunas que certas leis deixaram (MAUES; DUARTE; CARDOSO, 2018).

Ao Código Penal julgar aquele que comete crime cibernético, sendo assim, os crimes no Código Penal são figurados como, delitos cibernéticos próprios, esses dependem da internet para se concretizarem, o objetivo principal dos criminosos é violar as informações, o outro tipo são os delitos cibernéticos impróprios, esses para se concretizarem dependem da tecnologia, de softwares avançados (MAUES; DUARTE; CARDOSO, 2018).

A seguir vamos abordar sobre os crimes cibernéticos contidos no Código Penal, a princípio mencionaremos um pouco sobre a Calúnia, a Injúria e a Difamação, que são crimes descritos no capítulo V do Código Penal onde estão descritos os crimes contra a honra, esses crimes tem previsão legal no artigo 138 ao 140 do Código Penal (SANTOS; MARTINS; TYBUCSH, 2017).

O artigo 138 do Código Penal (BRASIL, 1940) é o que dispõe sobre a *calúnia*, e em seu tipo penal diz que, caluniar alguém é imputar a ela determinado fato definido como crime. O artigo 139 do Código Penal (BRASIL, 1940) dispõe sobre a *difamação*, e em seu tipo penal diz que, difamar alguém é imputar a ela algum fato ofensivo à sua reputação. O artigo 140 do Código Penal (BRASIL, 1940) dispõe sobre a *injúria*, e em seu tipo penal diz que, injuriar alguém é ofender alguém, direcionando essa ofensa a tal pessoa onde irá atingir a sua dignidade ou o seu decoro. Na mesma perspectiva o doutrinador Fernando Capez (2012, p.306) ressalta:

> Injuriar alguém se trata de um crime de ação livre. Todos os meios hábeis à manifestação do pensamento podem servir à injúria: a palavra oral ou escrita, a pintura, o gesto, etc.

Os crimes mencionados acima podem ocorrer tanto em meio físico como em meio digital e o artigo 141, §2º do Código penal, diz que se o crime for cometido

ou divulgado em quaisquer modalidades das redes sociais da rede mundial de computadores, aplicam-se a esses crimes o triplo a pena (MASSON, 2016).

No âmbito da internet, os crimes de calúnia e difamação, são ofensas que atingem à honra objetiva, quem pratica esses delitos tem como objetivo causar ofensa para um número grande de pessoas e não somente para a vítima. Já o crime de injúria, são ofensas que atingem à honra subjetiva, tal ofensa é direcionada para a própria vítima, um exemplo de calúnia que pode ser cometida através da internet é a fakenews (SANTOS; MARTINS; TYBUCSH, 2017).

Em seguida, vamos abordar sobre o crime de *ameaça*, está tipificado no artigo 147, do Código Penal e em seu tipo penal descreve que, ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave, ou seja, intimidar alguém, através da internet, causando a ela algum mal injusto, falando que vai matá-la ou afins é considerado crime cibernético, este crime acaba sendo muito comum em redes de conversa, como WhatsApp, Instagram, etc (MAUES; DUARTE; CARDOSO, 2018).

Outro crime contido no Código Penal é a *pornografia infantil*, o crime está tipificado nos artigos 241 e 241-A do Estatuto da Criança e do Adolescente, e no tipo penal do artigo 241 está descrito que, vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente (MAUES; DUARTE; CARDOSO, 2018).

Já no artigo 241-A, em seu tipo penal está descrito que, 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, sendo assim, o crime de pornografia infantil se caracteriza pelo ato de fotografar ou publicar cenas de sexo explícito que contenham crianças ou adolescentes, se enquadrando em crimes cibernéticos (MAUES; DUARTE; CARDOSO, 2018).

Em seguida, vamos falar dos crimes contra o patrimônio, primeiro vamos abordar sobre o crime de *estelionato*, ele encontra-se definido no artigo 171 do Código Penal, no seu tipo penal está descrito que, 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 (SANTOS; MARTINS; TYBUCSH, 2017).

No meio digital, a forma mais comum da pratica desta conduta delituosa é por meio da clonagem de sites ou envio de e-mails fakes que em via geral são relacionados a sites de bancos onde o usuário automaticamente digita seus dados bancários e por meio da internet os criminosos tem acesso a todos os dados e utilizam para fazer transferência do dinheiro, trazendo assim, grande prejuízo à vítima (SANTOS; MARTINS; TYBUCSH, 2017).

Temos também o crime de *divulgação de segredo*, previsto no artigo 153, do CP, no seu tipo penal está descrito que, divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem, sendo assim, revelar segredos de terceiros na internet ou divulgar algum documento confidencial que possa causar danos é crime, e pode ser considerado um crime cibernético (SANTOS; MARTINS; TYBUCSH, 2017).

No artigo 154-A do Código Penal, está tipificado o crime de *invasão de dispositivo informático*, e em seu tipo penal está descrito que, 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, é crime, e é considerado um crime cibernético (SANTOS; MARTINS; TYBUCSH, 2017).

Não podemos esquecer do crime de *pirataria*, sabemos que a criação e utilização da internet, trouxe diversas facilidades para os autores, como a divulgação de seus trabalhos e venda dos seus produtos, mas tem um ponto que ficou bastante

complicado para os mesmos, como o episódio da pirataria que é conhecida pelo download ou distribuição de conteúdo protegido por direito autoral sem a devid- autorização do autor (JESUS, 2016).

A Lei nº 9.610/98, atualizou e consolidou a legislação sobre direitos autorais, no seu artigo 26, VI, § 3º, onde proíbe o comércio ilegal de obras intelectuais por vias tecnológicas que não tenham autorização legal. Temos também a Lei nº 10.695/03 adequou o tipo penal do artigo 184 do Código Penal, que antes tratava apenas de violação do direito do autor, passando a abordar agora todas as outras questões conexas ao tema (JESUS, 2016).

Para César Bitencourt (2014, p.402), o crime de pirataria assim pode ser entendido da seguinte maneira:

> Essa previsão legal pode ainda não ser a ideal, mas já se oferece as condições mínimas para se começar a combater a pirataria da era cibernética. Infelizmente essas alterações não foram suficientes para combater esse crime, pois a falta de uma legislação específica, mais abrangente, faz com que a venda e distribuição de produtos não autorizados seja cada vez maior, causando, inclusive prejuízos aos cofres públicos.

E por último mais não menos importante, a Lei 12.737/12, essa lei famosa e conhecida como a Lei Carolina Dieckmann e trouxe algumas alterações ao Código Penal Brasileiro, onde foi tipificado alguns crimes de informática. Foi por meio do Projeto de Lei nº 2793/2011 quando a referida atriz teve o seu computador pessoal invadido por crackers que invadiram a sua privacidade e mais de 30 fotos íntimas foram publicadas na Internet sem qualquer restrição. Devido à grande publicidade que teve esse fato o projeto de Lei foi tramitado com urgência no Congresso Nacional (JESUS, 2016).

Essa lei inseriu ao Código Penal os artigos 154-A e 154-B sendo estes tipificados como “invasão de dispositivo Informático, que já foi abordado anteriormente. Esse artigo fortaleceu o direito a intimidade que está prevista na Constituição Federal em seu artigo 5º, inciso X (JESUS, 2016).

O legislador usou o termo dispositivo informático alheio para que este artigo continuasse sempre atual, assim, não foi taxativo em informar qual o dispositivo é passível de invasão, já que surgem vários tipos de dispositivos informáticos na atualidade. Neste sentido o entendimento do doutrinador Rogério Greco (2004, p. 146) é:

> Para que ocorra a infração penal sub examen, exige o tipo penal, ainda, que a conduta seja levada a efeito mediante violação indevida de mecanismo de segurança. Por mecanismos de segurança podemos entender todos os meios que visem garantir que somente determinadas pessoas terão acesso ao dispositivo informático, a exemplo do que ocorre com a utilização de login e senhas que visem identificar e autenticar o usuário, impedindo que terceiros não autorizados tenham acesso às informações nele contidas.

No Código Penal (BRASIL, 1940) e em leis esparsas no ordenamento jurídico brasileiro, temos muito ainda, sobre os crimes cibernéticos, neste tópico foi abordado os mais comuns e os mais utilizados atualmente na sociedade.

2.2– Sujeitos dos crimes

Nos crimes cibernéticos, é difícil comprovar de quem foi a autoria do crime, devido à ausência física do sujeito ativo, com isso surgiu a necessidade de classificar os sujeitos dos crimes de acordo com a especificação de cada um.

Então os crimes cibernéticos temos os seguintes sujeitos, em primeiro lugar temos os usuários, e sim, as vezes os próprios usuários praticam delitos informáticos e agem sem saber que essa conduta é crime, de exemplo temos, ao fazer uma publicação de uma imagem de terceiros em alguma rede social sem a devida autorização, invadindo a privacidade desse terceiro (ROSSINI, 2004).

Em segundo lugar temos os hackers, que são aquelas pessoas com grandes habilidades em computadores e que usam essas habilidades para melhorar softwares, segurança de sistemas internos de empresas, aplicativos. Em regra geral, são pessoas que usam esses conhecimentos em favor de empresas, para aumentar a segurança das mesmas, a probabilidade dessas pessoas se tornarem criminosos virtuais, é baixa, pois visam segurança na internet, evitando

os crackers invadem algum software para prejudicar o sistema interno de alguma empresa, etc (ROSSINI, 2004).

Em terceiro lugar, temos os crackers, esses são totalmente diferentes dos hackers, pois usam todo o seu conhecimento em tecnologia com intuito de prejudicar pessoas, sendo assim, eles são criminosos especializados em invadir segurança, invadir dispositivos eletrônicos de terceiros com objetivo de roubar dados, senhas, prejudicar o sistema interno de empresas, fazendo com o que os usuários percam todos os seus dados, e muitas vezes pedem resgate para "devolver" os dados (ROSSINI, 2004).

Em quarto lugar, temos os carder, que são pessoas que atuam na internet geralmente em grupo, o principal objetivo desses sujeitos é conseguir dados e senha de cartões de créditos para realizar fraudes via online, ou seja, são os famosos estelionatários, eles analisam que certos usuários são vulneráveis com seus dados e fazem clonagem dos dados para efetuarem compras online (ROSSINI, 2004).

Em quinto lugar, temos os vírus, que nada mais é que, programas instalados nos computadores que o infecta com objetivo de prejudicar desempenho e deixar o computador mais vulnerável a ataques de crackers. Geralmente, os vírus vêm em forma de anexo em e-mail, em mídias removíveis como pen drives e HD externo. Na maioria das vezes o usuário executa esses arquivos de forma inocente, sem saber que se trata de um vírus (ROSSINI, 2004).

Rafaela Pozzebon (2014, *online*) dar dicas de como manter o computador livre de ameaças virtuais:

> Utilizar senhas fortes, com letras e números alternados; trocar as senhas periodicamente; usar somente sistemas operacionais atualizados e seguros; sempre ter um bom antivírus atualizado no computador; não abrir anexos desconhecidos em e-mails, ou em mensagens em geral; não baixar arquivos em sites suspeitos; suspeitar sempre de qualquer arquivo enviado.

Neste tópico, foi abordado os sujeitos do crime cibernéticos, que são aquelas pessoas que podem praticar esse tipo de conduta delituosa.

2.3 – Análise de crimes cibernéticos

Neste tópico será abordada uma análise do crime cibernético de fraudes eletrônicas, mencionando aspectos relevantes sobre o tema, como os sujeitos desse crime agem para cometer este delito, e por fim trazer resumidamente sobre como esse crime é investigado.

O crime cibernético de fraude eletrônica tem aumentado consideravelmente no Brasil, principalmente as fraudes com cartões de crédito, devido à grandes movimentações do internet banking, que trouxe mais comodidade para fazer compras virtualmente, não apenas para esta finalidade, mais também podendo pagar boletos, fazer transferência, PIX e etc. Mas sabe-se que atualmente existem os crackers que utilizam programas maliciosos e sites que roubam os dados/informações dos computadores das vítimas, geralmente esses programas e sites, roubam dados como número do cartão, data de validade e o código de segurança (CASSANTI, 2014).

Habitualmente, o meio que os criminosos costumam a agir é enviando um e-mail à vítima e nele contém um link fraudulento, o objetivo do acesso ao link é o roubo dos dados das vítimas reproduzindo um site do governo, site de algum banco conhecido ou site de alguma empresa grande e famosa, e os crackers simulam os e-mails de uma forma que induz a vítima a achar que foi sorteada de algum prêmio, ou que a conta dela foi bloqueada, que o FGTS foi sacado, fatos esses que fazem a vítima acessar os links maliciosos fazendo com que preencha formulários inserindo dados pessoais capazes de coletar tais informações para os criminosos (WENDT; JORGE, 2012).

Esse tipo de golpe que os criminosos virtuais praticam são conhecidos como phishing scam, e a investigação deste delito é bem criteriosa, isto ocorre porque para se investigar esses crimes tem que haver um preparo do ambiente

virtual investigatório, portando é essencial instalar um programa no computador chamado máquina virtual, esse programa traz a possibilidade de instalação de programas/sistemas que fazem execução desses programas que roubam dados (WENDT; JORGE, 2012).

Acerca deste tema, os doutrinadores Emerson Wendt e Higor Vinicius Nogueira Jorge (2012, p.108), dizem a respeito da investigação do crime de fraude com cartões de crédito:

> O primeiro passo da investigação em caso de fraude com cartões de crédito é oficiar a instituição bancária para obtenção do número IP, data, hora e padrão GMT, e ouvir a explicação da vítima de como ocorreu a compra indevida, a fim de identificar o método utilizado pelo criminoso para fraudar o cartão de crédito.

Neste tópico foi analisado o crime cibernético de fraude eletrônica, abordando aspectos relevantes do tema, o procedimento de investigação e etc.

Nesse capitulo, foi abordado a priori, os crimes cibernéticos dentro do Código Penal (BRASIL, 1940), realizando um breve apanhado dos conceitos desses crimes, trazendo todos os aspectos relevantes do tema, bem como, apresentando as lacunas que existem atualmente no ordenamento jurídico brasileiro em relação aos crimes cibernéticos.

Posteriormente, foi abordado sobre os sujeitos que cometem os crimes virtuais, mencionando como esses sujeitos agem para praticar o crime, e como a sociedade pode fazer para evitar ser vítima desse delito.

E para finalizar este capitulo, foi realizada uma análise de um crime cibernético, o crime de fraude eletrônica, no qual perspectivas importantes foram abordadas, trazendo além do mais sobre a investigação do crime de fraude eletrônica sobre aspecto.

CAPÍTULO III – CRIMES CIBERNÉTICOS E LEI GERAL DE PROTEÇÃO DE DADOS

Neste capitulo, será abordado acerca dos crimes cibernéticos e a Lei Geral de Proteção de Dados (BRASIL, 2018), sendo feita uma análise da conexão dos crimes cibernéticos com a Lei Geral de Proteção de Dados. Também será mencionado a importância da Lei Geral de Proteção de Dados no combate aos Crimes Cibernéticos, e por fim será abordado quais são as precauções trazidas pela Lei Geral de Proteção de Dados para que a sociedade não se torne vítima de delitos cibernéticos.

É importante recordar dois pontos principais, sendo eles, o que é crime cibernético e qual é o objetivo da Lei Geral de Proteção de Dados (BRASIL, 2018). Crime Cibernético ocorre quando criminosos utilizam de computadores, e/ou uma rede de computadores e/ou dispositivos celulares conectados a uma rede de internet para praticar delitos.

Já a Lei Geral de Proteção de Dados (BRASIL, 2018), tem como objetivo conceber segurança jurídica a sociedade, realizando padronizações de regulamentos, e com isso promovendo maior proteção de dados pessoais e dados sensíveis.

3.1- Conexão dos Crimes Cibernéticos com a Lei Geral de Proteção de Dados

Os crimes cibernéticos ou cibercrimes são as execuções ilícitas cometidas na web, através de dispositivos eletrônicos, como computadores e celulares. Alguns

desses criminosos são hackers que usam de modalidades avançadas e outros hackers que utilizam modalidades de golpes mais simples, comumente, os dados roubados são informações pessoais e dados bancários (CASSANTI, 2014).

A Lei Geral de Proteção de Dados tem como referencial a GDPR (General Data Protection Regulation), uma ordenação europeia, que, de igual natureza, é baseada nos direitos fundamentais de liberdade, privacidade e do livre desenvolvimento da personalidade da pessoa natural, para estabelece normas e procedimentos com o intento de coletar e armazenar dados de pessoas físicas com maior segurança e transparência, penalizando com multas as empresas que descumprirem as determinações estabelecidas (LOPES, 2021).

A Lei Geral de Proteção de Dados define o que pode ser considerado dados pessoais e explica que alguns deles estão sujeitos a cuidados ainda mais específicos, como os dados pessoais sensíveis e dados pessoais sobre crianças e adolescentes. A lei deixa claro que, todos os dados tratados, tanto no meio físico quanto no digital, estão sujeitos à regulação (LOPES, 2021).

Consoante o que alude o doutrinador Alan Moreira Lopes, acerca da importância de saber sobre o que é pessoa natural e dados sensíveis no ponto de vista da LGPD:

> A importância dada ao esclarecimento do que é “pessoa natural” e “dados sensíveis”, demonstra a preocupação do legislador em proteger o cidadão em toda a sua individualidade sem deixar de amparar a coletividade diante da explícita descrição normativa. Quando discorremos sobre proteção de dados pessoais, torna-se imperioso entender que para proteger é necessário traçar um paralelo com a segurança pública, com essa nova modalidade de crimes é extremamente relevante tutelar os dados pessoais numa ótica digital (LOPES, 2021, p. 34).

Mundialmente, tem-se ampliado os golpes ocorridos por meio digital, numa evolução de mecanismos para subtrair de outrem vantagens e privilégios. Incorporou-se ao cotidiano dos crimes presenciais e ataques físicos essa nova modalidade de crimes virtuais (LOPES, 2021).

Além disso, a Lei Geral de Proteção de Dados estabelece que não importa se a sede de uma empresa ou o centro aonde ela armazena os dados, estão localizados no Brasil ou no exterior: se há o processamento de informações sobre pessoas, brasileiras ou não, que estão no território nacional, sempre deverá prevalecer a Lei Geral de Proteção de Dados, devendo ser observada em qualquer hipótese (LOPES, 2021).

Dessa forma, fica bem claro que a lei supracitada, autoriza também, o compartilhamento de dados pessoais com organismos internacionais e com outros países, desde que observados os requisitos nela estabelecidos (LOPES, 2021).

Na prática, e de forma resumida, a Lei Geral de Proteção de Dados impede que as empresas mantenham dados de terceiros, como clientes, fornecedores e funcionários, em suas bases, sem o devido consentimento, tratando assim, dados pessoais, como nomes, números de documentos, endereço físico e eletrônico etc (LOPES, 2021).

Porém, há alguns dados pessoais que são considerados sensíveis e exigem condições de tratamento mais específicas. Sendo eles: dados genéticos ou biométricos, ou seja, dados que nos identificam como seres humanos; dados relativos à vida sexual ou orientação sexual da pessoa; convicções religiosas ou filosóficas; informações sobre a saúde; origem racial ou étnica; opiniões políticas; e filiação sindical (TEFFÉ, 2022).

Em suma, os dados sensíveis são os dados dos cidadãos e que, por princípios éticos, não podem ser vazados. Como exemplo de dados pessoais sensíveis, é que se um indivíduo é homossexual ou um indivíduo é filiada a um partido político, essa informação pertence a ela e não pode ser divulgado por terceiros. Então, com a chegada da Lei Geral de para que os estabelecimentos comerciais possam manter um cadastro de clientes, é necessária uma autorização expressa de cada pessoa para isso (TEFFÉ, 2022).

A Lei Geral de Proteção de Dados, entrou em vigor em setembro de 2020, porém as multas impostas pela lei passaram a ser válidas no mês de agosto de 2021. Contudo, os estabelecimentos em geral que não cumprirem com a determinação estão correndo risco de serem multadas. Sendo assim, as empresas que manuseiam dados de clientes de forma indevida poderão ser multadas com um valor de até 2% do faturamento total da pessoa jurídica, limitado a R$ 50 milhões (LOPES 2021).

Além das multas, os estabelecimentos pode ser bloqueado ou sofrer perda dos seus dados. As sanções são muito rígidas e a multa bastante alta, isso foi imposto para que as empresas corram atrás para se adaptar (TEFFÉ, 2022).

E por fim, para destacar sobre a conexão da Lei Geral de Proteção de Dados com os crimes cibernéticos, fica evidente que com essas medidas torna a vida virtual mais segura, pois atualmente vivemos em um mundo em que a maior parte do nosso dia se concentra na internet, usamos para trabalhar, estudar, e como a tecnologia vem evidenciando cada vez mais o uso da internet, a nova legislação veio para combater a prática de atos praticados por meio virtual, exigindo uma melhor maturidade da segurança da informação, tornando as empresas menos vulneráveis aos criminosos digitais e ao vazamento de dados pessoais (TEFFÉ, 2022).

3.2– A importância da Lei Geral de Proteção de Dados no combate aos Crimes Cibernéticos

Os criminosos digitais observaram na Lei Geral de Proteção de Dados uma forma a mais de pressionar as empresas a pagarem pelo resgate de dados, quando invadem os computadores das empresas e roubam os dados de colaboradores, clientes e parceiros, e além do mais expõem as falhas de segurança da informação da empresa, trazendo assim, uma falha na adequação às exigências da lei, gerando grandes possibilidades de serem multadas pela Agência Nacional de Proteção de Dados (LOPES, 2021).

Na maioria dos casos, o que acaba ocorrendo ataques de roubo de dados, feito por criminosos, por meio de criptografia, usando como refém arquivos pessoais da própria vítima, e ainda mais, cobrando resgate para reconstitui o acesso a esses dados, e esses ataques são conhecidos como Ransomware, os criminosos não fazem nada com os dados, apenas os mantêm em sua posse e bloqueiam o acesso aos dados, como essa conduta dos criminosos, a empresa fica a mercê deles (LOPES, 2021).

Como as multas da Lei Geral de Proteção de Dados são muito altas e podem chegar a R$ 50 milhões, inúmeras empresas acabam caindo na chantagem desses criminosos, observando que, é mais vantajoso ceder às chantagens dos criminosos e pagar menos do que pagaria na multa (LOPES, 2021).

Então, é suma importância, se adequar o quanto antes, de maneira disciplinada pela Lei Geral de Proteção de Dados. Como isso, fica garantido que a empresa irá cumprir com a legislação, melhorando a maturidade da segurança do ambiente de TI, educando os colaboradores nas melhores práticas de segurança.

Por intermédio dessas circunstancias, é indicado que as empresas, se adequem o mais breve possível para evitar que os crimes cibernéticos ocorram. Dessa maneira, as empresas devem optar em ter um antivírus eficaz e ter sistemas de proteção de dados (TEFFÉ, 2022).

De acordo com o que disciplina a Lei Geral de Proteção de Dados, o objetivo da lei pode ser resumido em alguns principais pontos, sendo eles:

> Fortalecer os direitos dos indivíduos; capacitar os atores envolvidos no processamento de dados; aumentar a credibilidade da regulamentação por meio de uma cooperação entre as autoridades de proteção de dados (BRASIL, 2018, *online*).

Com o surgimento da Lei Geral de Proteção de Dados, forneceu as empresas mais visibilidade sobre os dados que estão sendo coletando. O princípio básico da lei é que as empresas conheçam os dados de que dispõem e garantam

que estão sendo processados corretamente garantindo segurança (FLOWTI, 2021, *online*).

As empresas que já estão em conformidade com Lei Geral de Proteção de Dados têm em mente que, o elemento básico que uma empresa preciso para se adequar, é ter um excelente programa de segurança da informação (FLOWTI, 2021, *online*).

A Lei Geral de Proteção de Dados alterou a equação financeira das organizações, estabelecimentos comerciais, no que tange ao risco que tem sobre a privacidade, e isto fez com que as empresas pensassem de uma forma mais holística sobre os riscos e como investir na melhoria dos controles e governança de privacidade (TEFFÉ, 2022).

3.3– Precauções trazidas pela Lei Geral de Proteção de Dados para que a sociedade não se torne vítima de delitos cibernéticos

Com a entrada da vigência da Lei Geral de Proteção de Dados, um horizonte bastante inovador em frente as empresas, aumentando sobremaneira suas responsabilidades e exigindo uma adequação nos processos de condução e proteção de dados. O universo virtual pode até parecer oculto e imperceptível, mas não assegura por longo período o anonimato. Deixamos rastros, por onde quer que naveguemos (FLOWTI, 2021, *online*).

Em termos, a Lei Geral de Proteção de Dados (BRASIL, 2018), considerando sua contribuição para a segurança pública e defesa nacional e atividades investigativas. A prática generalizada de crimes cibernéticos está em ascensão, prejudicando a sociedade e prejudicando diretamente a segurança pública. Consequentemente, em muitos casos, intrusões de hackers em sites de propriedade direta da administração ou de agências independentes e governamentais ocasionaram danos consideráveis à defesa nacional. Veja a seguir como a Lei Geral de Proteção de Dados, pode implicar na segurança pública:

> A Lei Geral de Proteção de Dados busca abranger tutela em vários ramos do direito, sendo um dos mais corriqueiros, o Direito Penal. Sendo indispensável para Segurança Pública, não só ao combate como também a prevenção de delitos. Essa lei, além de combater e punir os crimes referentes a invasão dos dados pessoais, atua na punição de crimes já conhecidos como injúria racial, xenofobia, homofobia, pedofilia e tantos outros cometidos através das redes sociais (FLOWTI, 2021, *online*).

Consequentemente, a Lei Geral de Proteção tem o intuito de eliminar a prática de crimes virtuais. Dessa forma, conforme mencionado, os vazamentos e roubos de dados pessoais tendem a ter significativa queda, pois a Lei além de ter função preventiva e punitiva, também exerce caráter didático deixando a população ciente dos riscos (FLOWTI, 2021, *online*).

Destarte, é válido frisar acerca das questões correlacionadas a Segurança Pública virtual, mesmo ocorrendo o evidente crescimento no combate aos crimes cibernéticos, acontece de forma muito devagar, enquanto os criminosos virtuais são muito ágeis. Logo, demanda mais tempo para preparar todos os envolvidos, sendo assim, podermos afirmar que a Segurança Pública está em formação constante para diferir essas modalidades de crimes (FLOWTI, 2021, *online*).

Alguns juristas, composto pelos Ministros do Superior Tribunal de Justiça (STJ) Nefi Cordeiro, Antônio Saldanha Palheiro e relatada pela Professora Laura Schertel, da Universidade de Brasília (UnB), e seus pares, apresentam o anteprojeto, que visa equiparar a necessidade do Estado em proteger dando segurança e ao mesmo tempo compatibilizando e assegurando direitos subjetivos num espaço delimitado para as investigações, visando um bem comum. Coloca-se em relevo a eminente necessidade de proteger à vítima e a sociedade (PSAFE, 2017, *online*).

O anteprojeto tem como finalidade limitar a liberdade de expressão, a livre manifestação do pensamento sem atropelar as quatro linhas da Constituição. Assim, atitudes antiéticas que ferem o código penal, nossa Carta Magna, e aos bons costumes, a luz da imparcialidade serão réprobos em seus objetos. De acordo com o que disciplina o artigo 144, caput da Constituição Federal:

> A segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio (BRASIL, 1988, *online*).

Dentre uma linha imaginária podemos apreciar que a Segurança Pública possui um lugar importante no que tange a proteção de dados, a quebra de sigilo, a investigação criminal, dentre outros, é imperativo para atuação das autoridades, até mesmo para beneficiar uma justa proteção social (PSAFE, 2017, *online*).

Todavia, atrelada ao quanto será necessário o acesso a certos dados, o Estado em sua inteligência busca alternativas cientificas para encontrar soluções e melhor servir a população. É um discurso inserido de debates, longe de se esgotar. Sabemos que muitas vielas serão percorridas até cruzarmos a linha de chegada (PSAFE, 2017, *online*).

O magistrado Ney Bello, trouxe uma analogia entre o que é considerado como liberdade e o que é considerado privacidade:

> Acerca de algumas restrições dos direitos fundamentais, contudo a respeitar os limites da proporcionalidade. É necessária uma aproximação do Estado sem que descomponha as vestes da autonomia de direitos. Essa autoridade no seu sério papel, tem por oficio a busca de soluções (Brasil, 2021, online).

Alguns estudiosos da Tecnologia da Informação costumam a dar dicas de como será a questão envolvendo os crimes cibernéticos, no qual atingem uma grande quantidade de usuários, sendo assim eles alertam, sempre estar em alerta e investir em proteção. Em suma, não adianta colocar o melhor e mais atualizado antivírus se vai clicar em qualquer anexo de algum e-mail desconhecido e sem a mínima confiabilidade. Em vista disso, veja a seguir algumas dicas que o site Psafe, publicou acerca dos cuidados que deveremos ter para não sermos vítimas de delitos cibernéticos, sendo eles:

> Use senhas fortes, os especialistas avisam: não é indicado colocar senhas de sequência fácil, tais como 123456. É claro que é possível utilizar uma sequência de números, letras, símbolos e demais caracteres, mas não é nada bom que ela seja quase que perceptível mesmo para um desconhecido, a senha serve para resguardar muitos dos seus dados tanto no seu computador quanto na internet. Desde e-mails até cartões de créditos e internet banking, a senha é a sua chave de acesso para se

> movimentar online. Portanto, é importante que ela garanta sua segurança. Alguns servidores exigem longas senhas com números, letras maiúsculas e minúsculas, além de símbolos aleatórios, o que, no fim das contas, pode fazer com que você construa uma senha mais ou menos assim: jKuiL87KtS#98*e76; jamais clique em links ou anexos de e-mails desconhecidos. É praxe, mas vale reforçar: a sua segurança depende das suas atitudes e atividades tanto no seu computador quanto nas redes (internet) que você frequenta. A abertura de arquivos desconhecidos (tais como de supostas premiações ou depósitos milagrosos) esconde um grande risco de se ter o computador ou a rede hackeados; mantenha o antivírus atualizado, agora que você já sabe que deve ter uma senha forte e manter-se longe de e-mails duvidosos, é preciso ressaltar a relevância de deixar o seu computador sempre atualizado. Tais quais os crimes cibernéticos, os vírus e as ameaças online evoluíram e seguem se aprimorando. Então, é importante verificar se um site é legítimo antes de preencher suas informações é preciso pesquisar, o que pode dar certo trabalho. No entanto, esse é o melhor caminho a seguir na hora de verificar se um site é seguro ou não; mantenha seu software e seu sistema operacional atualizados, garantindo as mais recentes correções de segurança para proteger seu computador; use antivírus e mantenha-o também atualizado, esse tipo de proteção permite que você verifique, detecte e remova ameaças antes mesmo delas se tornarem um problema; senhas fortes também é uma solução para esse problema e não as registre em lugar algum; quando o e-mail for para o spam, nunca abra seus anexos e nem clique em links de sites desconhecidos; não forneça suas informações pessoais, a menos que tenha certeza com quem está falando e entre em contato diretamente com as empresas para confirmar pedidos suspeitos; fique sempre atento aos seus extratos bancários, qualquer transação incomum, acione seu banco que irá investigar uma ação fraudulenta (PSAFE, 2017, *online*).

E por fim, conclui-se que, é extremamente necessário ter muita atenção em tudo que fazemos por meio digital para não sermos vítimas de nenhum tipo de crime cibernético, pois estamos constantemente vulneráveis a ataques de criminosos.

CONCLUSÃO

O presente trabalho abordou que, o Direito Penal está ligado em muitos aspectos com as condutas criminosas na esfera da internet, e com a evolução da tecnologia, a tendência é que cresça cada vez mais o número de usuários na rede, visto que, a sociedade se tornou dependente da internet, necessitando manter-se conectada na maior parte do tempo, o que ocasiona o crescente número de delitos cibernéticos por meios digitais.

Com isso, o direito se atualiza constantemente para acompanhar esse progresso, tipificando os crimes cibernéticos. Haja vista que, é imprescindível que o legislador crie tipos penais que englobe as práticas ilícitas praticadas na internet, ressaltando ainda que, como a legislação atual deixa um pouco a desejar no quesito punição, tornando ainda mais difícil identificar os crimes ocorridos pela internet, impactando na demora para se chegar ao autor dessas condutas ilícitas.

Destarte, observa-se que apenas criar leis punitivas para esse crime não basta, sendo necessário que o poder judiciário seja capaz de tornar essas leis eficazes, formulando uma execução competente do poder de polícia, e com isso automaticamente, fazendo com que os cidadãos possam ter ciência dessa lei e de suas sanções, e aos poucos acabando com a mentalidade que se tem atualmente, onde pensam que a internet é terra sem lei, sem limites.

Para obstar as condutas cibernéticas e golpes em meios virtuais, um dos métodos criados foi a Lei 13.709/2018, lei esta que versa sobre a Lei Geral de Proteção de Dados (BRASIL, 2018), e que entrou em vigor no Brasil em agosto de

2021, com o intuito de guiar empresas que retém dados de clientes, passando a punir de forma pecuniária essas empresas que viabilizam dados sigilosos.

Pelos motivos acima expostos, observamos a suma importância que a LGPD trouxe para o ordenamento jurídico, sabe-se que, os criminosos digitais agem com o intuito de roubar os dados pessoais de terceiros, dados pessoais de clientes de empresas para proveito próprio, entretanto, a referida lei tenta reduzir essa situação, trazendo requisitos para ser cumpridos tanto por pessoa física como por pessoa jurídica, tornando assim, os dados mais seguros.

REFERÊNCIAS

ALVES, L. B. M.; BERCLAZ, M. S. **Ministério Público em Ação**. In. (Coord.) GARCIA, L. M. Coleção Carreiras em Ação. 6ª ed. rev., ampliada e atualizada. Salvador: Juspodivim, 2017.

BARROS, M. A. de.; GARBOSSA, D. D.; CONTE, C. P. Crimes informáticos e proposição legislativa: considerações para uma reflexão preliminar. **Revista dos Tribunais**. v. 865, 2007.

BITTENCOURT, R. P. P. **O anonimato, a liberdade, a publicidade e o direito eletrônico**. 2016, Disponível em: https://rodolfoppb.jusbrasil.com.br/artigos/371604693/o-anonimato-a-liberdade-a-publicidade-e-o-direito-eletronico. Acesso em: 14 mai de 2022.

BOITEUX, L. Crimes informáticos: **reflexões sobre política criminal inseridas no contexto internacional atual**. Doutrinas Essenciais de Direito Penal. v. 8, 2010.
BRASIL, Decreto – **Lei nº 2.848 de 07 de dezembro de 1940**. Diário Oficial [da] República Federativa do Brasil, Poder Legislativo, Brasília, DF, 07 dez. 1940. Disponível em: https://www2.camara.leg.br/legin/fed/declei/1940-1949/decreto-lei-2848-7-dezembro-1940-412868-norma-pe.html. Acesso em: 09 out. 2022.

BRASIL, **Lei nº 13.709 de 14 de agosto de 2018**. Diário Oficial [da] República Federativa do Brasil, Poder Legislativo, Brasília, DF, 14 ago. 2018. Disponível em: https://www2.camara.leg.br/legin/fed/lei/2018/lei-13709-14-agosto-2018-787077-norma-pl.html. Acesso em: 09 out. 2022.

BRASIL. **Constituição da República Federativa do Brasil**. Brasília: Senado, 1988. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/518231/CF88_Livro_EC91_2016.pdf. Acesso em: 09 out. 2022.

CASSANTI, M. de O. **Crimes virtuais, vítimas reais**. 1. ed. Rio de Janeiro: Brasport, 2014.

DAOUN, A. J. **Os novos crimes de informática.** 1999. Disponível em http://jus2.uol.com.br/doutrina/texto.asp?id=1827. Acesso em: 23 mai de 2022.

DIZARD Jr., W. **A nova mídia:** a comunicação de massa na era da informação. Rio de Janeiro: Jorge Zahar Ed., 2000.

ELEUTÉRIO, P.M.S.; Machado, M.P. **Desvendando a computação forense**. 1ª ed. São Paulo: Novatec, 2011.

FLOWTI. **A importância da LGPD no combate aos cibercrimes**. Brasil, 12 nov. 2021. Disponível em: https://flowti.com.br/blog/a-importancia-da-lgpd-no-combate-aos-cibercrimes. Acesso em: 20 out. 2022.

GUIZZO, É. **Internet:** O que é, o que oferece, como conectar-se. 1ª ed. São Paulo. Editora Ática: 1999.

LOPES, A. M. **Direito Digital e LGPD na Prática**. São Paulo: Editora Rumo Jurídico, 2021.

PAESANI, L. M. **Direito e Internet:** liberdade de informação, privacidade e responsabilidade civil. 1ª ed. São Paulo, Ed. Atlas, 2000.

PSAFE. **Ataques cibernéticos: o que é e como se proteger**. Brasil, 28 set. 2017. Disponível em: https://www.psafe.com/blog/ataques-ciberneticos-como-se-proteger/. Acesso em: 14 out. 2022.

ROSA, F. **Crimes de Informática**. Campinas: Bookseller, 2002.

ROSSINI, A. E. de S. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004.

TEFFÉ, C. S. de. **A importância da LGPD no contexto da inteligência de dados**. ITS, Rio de Janeiro/RJ, 2022. Disponível em: https://itsrio.org/pt/artigos/a-importancia-da-lgpd-no-contexto-da-inteligencia-de-dados/. Acesso em: 14 out. 2022.