UNIATENAS

LUCAS BELTRÃO DA SILVA

CRIMES CIBERNÉTICOS: prevenção e combate estatal

Paracatu

2021

LUCAS BELTRÃO DA SILVA

CRIMES CIBERNÉTICOS: prevenção e combate estatal

Monografia apresentada ao Curso de Direito Do Centro Universitário Atenas, como requisito parcial para obtenção do título de Bacharelem Direito.

Área de Concentração: Legislação Penal.

Orientador: Prof. Msc. Tiago Martins da Silva

Paracatu
2021

LUCAS BELTRÃO DA SILVA

CRIMES CIBERNÉTICOS: prevenção e combate estatal

Monografia apresentada ao Curso de Direito Do Centro Universitário Atenas, como requisito parcial para obtenção do título de Bacharelem Direito.

Área de Concentração: Legislação Penal.

Orientador: Prof. Msc. Tiago Martins da Silva

Banca Examinadora:
Paracatu- MG, 08 de Junho de 2021.

Prof. Msc. Tiago Martins Silva
UniAtenas

Prof.ª Msc. Amanda Cristina de Souza
UniAtenas

Prof. Msc. Edinaldo Junior Moreira
UniAtenas

Dedico este trabalho aos meus pais e a minha irmã, por acreditarem na minha realização. A minha namorada que sempre me apoiou e incentivou. E a todos os professores em que tive o prazer de estarem presentes comigo ao longo dessa caminhada.

AGRADECIMENTOS

Queria agradecer primeiramente a Deus que permitiu que tudo isso acontecesse, ao longo de minha vida e não somente nestes cinco anos como universitário, mas que em todos os momentos é o maior mestre que pude conhecer. A esta instituição, direção e administração que oportunizaram a janela que hoje vislumbro um horizonte superior, contagiada pela pura confiança do mérito e ética aqui presente. Ao meu querido orientador Msc. Thiago Martins Silva pelo carinho dedicado a mim, pelo suporte no pouco tempo que lhe coube, pelas suas orientações, correções e incentivos, deixo o meu muito obrigado! A todos os professores que lecionaram, por me proporcionarem o conhecimento, por tanto que se dedicaram a mim, não somente por terem me ensinado, mas por terem me feito aprender. A palavra mestre, se encaixa perfeitamente a vocês, aos quais sem nominar terão os meus eternos agradecimentos.

Em especial a minha mãe Elane, heroína que me deu apoio, incentivo nas horas difíceis, de desânimo e cansaço. Ao meu pai Belchior, que apesar de todas as dificuldades me fortaleceu e sempre esteve ao meu lado, obrigado por seu companheirismo pois para mim foi extremamente importante. À minha irmã e madrinha Thaciane, que não mediu esforços para me ajudar, agradeço por todas as dicas, incentivos e ademais ajudas concedidas a mim. À minha namorada Lauane, que assim como eu sabe o quanto é exaustiva essa caminhada e que mesmo nos momentos de minha ausência dedicada aos meus estudos, trabalhos, sempre foi companheira e paciente. Não poderia deixar de agradecer também ao meu primo e colega de estudos Alan, que desde o início me acompanhou neste sonho, pactuamos a nunca deixar o outro a desistir dessa caminhada árdua e hoje aqui estamos com muita alegria obtendo a nossa graduação.

Obrigado, meus queridos amigos Matheus, Iago, Carlos, Lara, Mariane, Dyefferson, pela amizade formada aqui na faculdade e que eu espero que se estenda pelo resto da vida. Desejo muito sucesso a vocês. Enfim, agradeço à todos os meus caros colegas de curso, juntos nós brilhamos, e também aqueles que direta ou indiretamente fizeram parte da minha formação. Isso é só a primeira etapa de mais um sonho a ser realizado.

“Quem tem medo da escalada, não merece o topo da montanha!”

(Felipe Titto)

RESUMO

A presente monografia tem por intuito, esclarecer dúvidas e requintar a compreensão no tocante ao universo dos crimes eletrônicos, os quais estão se tornando mais frequentes. No Brasil, os ataques cibernéticos estão cada dia mais evoluídos e sofisticados. A fim de erradicar esse problema e proteger os usuários que eventualmente pudessem ser vítimas desses crimes, foram elaboradas leis que inicialmente se mostraram ideias promissoras, mas que com o tempo se revelaram ineficientes no combate desses delitos. Ao decorrer do presente trabalho serão abordados os aspectos históricos e conceituais dos crimes cibernéticos, será informado quais são as normas abrangentes aos crimes virtuais, e ainda dentro da perspectiva do estudo monográfico será exposto uma série de instruções, medidas assecuratórias para se proteger do mundo dos cibercrimes.

Palavras chave: crimes eletrônicos, cibercrimes, combate, ineficientes.

ABSTRACT

This monograph aims to clarify doubts and refine understanding regarding the universe of electronic crimes, which are becoming more frequent. In Brazil, cyber attacks are increasingly evolved and sophisticated. In order to eradicate this problem and protect users who might eventually be victims of these crimes, laws were drafted that initially showed promising ideas, but which in time proved to be ineffective in combating these crimes. Throughout the present work, the historical and conceptual aspects of cyber crimes will be addressed, the comprehensive norms for cyber crimes will be informed, and even within the perspective of the monographic study, a series of instructions, security measures to protect yourself from the cybercrime.

Keywords: electronic crimes, cybercrimes, combat, inefficient.

SUMÁRIO

1. INTRODUÇÃO 10
1.1 PROBLEMA 11
1.2 HIPÓTESE DE ESTUDO 11
1.3 OBJETIVOS 11
1.3.1 OBJETIVO GERAL 11
1.3.2 OBJETIVOS ESPECÍFICOS 11
1.4 JUSTIFICATIVA 12
1.5 METODOLOGIA DO ESTUDO 12
1.6 ESTRUTURA DO TRABALHO 12
2. CIBERCRIMES E ATUAÇAO ESTATAL 14
2.1 EVOLUÇÃO HISTÓRICA 14
2.2 ASPECTOS CONCEITUAIS DOS CRIMES CIBERNÉTICOS 15
2.3 A PREVENÇÃO E O COMBATE DO ESTADO AOS CIBERCRIMES 16
3. TIPOS PENAIS, DESDOBRAMENTOS DA PRÁTICA DESTE CRIME 20
3.1 SUAS CLASSIFICAÇÕES E MODALIDADES 20
3.1.1 INVASÃO E PRIVACIDADE 21
3.1.3 FRAUDES VIRTUAIS 23
3.1.4 CRIMES CONTRA A HONRA 24
3.1.5 PORNOGRAFIA INFANTIL 25
3.1.6 ESTELIONATO 27
4. LEGISLAÇÃO CORRESPONDENTE 28
4.1 LEI DOS CRIMES CIBERNÉTICOS (LEI Nº 12.737/12) 28
4.2 MARCO CIVIL DA INTERNET (LEI Nº12.965/14) 31
4.3 AMPLIAÇÃO DE PENAS PARA CRIMES CIBERNÉTICOS (LEI Nº 14.155/2021) 314
5. CONSIDERAÇÕES FINAIS 36
REFERÊNCIAS 37

INTRODUÇÃO

O avanço tecnológico proporcionou muitas facilidades, comodidades e podemos dizer que até se tornou um “passatempo” para a sociedade contemporânea, se tornou, nos dias atuais, um verdadeiro fenômeno que modificou e remodelou sociedades em diversas áreas. (CASTELLS, 2019). Todavia, abriu várias brechas para a prática de delitos, chamados de crimes virtuais ou cibernéticos.

Podendo destacar que atualmente, essa prática delituosa aumentou de forma preocupante, consequência do isolamento causado pelo surgimento do vírus, COVID-19. É importante destacar que, independentemente do nível social, cultural, todos os usuários, estão passíveis de sofrer algum tipo de crime virtual. O problema é que, por muitas vezes quanto maior o nível de exposição de informações pessoais, maior o risco de sofrer algum golpe. (ROZA, 2016).

Conforme o que vem sendo exposto na literatura, cada dia mais vem crescendo os números de pessoas que acessam a internet, a cada dia são criadas mais de mil homepages por dia, o que acontece é que os usuários que ali se encontram estão sujeitos aos mais variados crimes, estes, que não encontram barreiras para perpetuar-se por toda a rede, deixando estragos imensos na vida dos internautas de boa-fé (PINHEIRO, 2010).

O presente trabalho monográfico vem com a ideia central de elencar todas as modalidades dos crimes virtuais, de modo a abordar conceitos de internet, elencando um rol de condutas criminosas pela internet, evidenciando os percalços causados pela falta de uma regulamentação específica acerca do tema e apontando peculiaridades sobre mecanismos de investigação e obtenção de provas, além de também indagar a forma que o Estado poderia efetivar o aparato legal contra a prática dos crimes cibernéticos, acompanhando o desenvolvimento tecnológico. Identificando ainda, se o direito penal brasileiro está totalmente adequado para as realidades da sociedade moderna, quando o assunto é crimes virtuais. (MEIDEROS, 2020)

1.1 PROBLEMA

O Estado tem aparato necessário para o combate e prevenção das condutas delituosas praticadas pela internet?

1.2 HIPÓTESE DE ESTUDO

Os legisladores brasileiros precisam produzir leis próprias para essa prática de delito, sendo essa modalidade um crime como qualquer outro tipificado no código penal brasileiro, tendo altos índices de impunidade por não ter a legislação específica. É preciso que o poder legislativo evolua junto com a tecnologia, a sociedade brasileira carece que os legisladores coloquem o código penal para caminhar simultaneamente com as necessidades que surgem por causa da constante evolução. Ademais, poderia ser criado um canal para as denúncias, criar delegacias especializadas sobre este assunto, e um melhor treinamento e capacitação dos seus agentes para agir sobre este crime.

1.3 OBJETIVOS

1.3.1 OBJETIVO GERAL

Analisar o aparato necessário que o Estado tem aparato para o combate e prevenção das condutas delituosas praticadas pela internet.

1.3.2 OBJETIVOS ESPECÍFICOS

a) Discorrer sobre a evolução histórica e conceito dos crimes cibernéticos
b) Verificar as espécies de crimes virtuais
c) Analisar a Legislação e projetos de leis sobre os crimes virtuais, a forma que o Estado pode promover a efetividade do aparato legal, atuando no combate e prevenção das condutas delituosas praticadas por meio da internet

1.4 JUSTIFICATIVA

A matéria de estudo é de suma importância pois se trata de um dos crimes mais praticados na atualidade e que tem a tendência de aumentar ainda mais os casos. Atualmente, devido ao isolamento social decorrente da epidemia de COVID-19, as pessoas saíram das ruas e se conectaram ao mundo virtual, e hoje crimes como furto, roubo, deram lugar ao desenvolvimento de novas práticas de crimes, como os crimes cibernéticos. Como a internet está sempre evoluindo e sendo sempre buscada por todos, acaba chamando a atenção de criminosos para atuar e estar efetuando golpes por este meio. Por isso existe a necessidade de tipificar os crimes cibernéticos, para uma melhor efetividade na segurança social, uma vez que os ciber crimes não param, e não contendo leis específicas, a dificuldade em definir a competência, e de identificar o sujeito do crime, acabam se concretizando em muitas impunidades.

1.5 METODOLOGIA DO ESTUDO

A pesquisa a ser realizada neste projeto classifica-se como descritiva e explicativa. Isso porque busca proporcionar maior compreensão sobre o tema abordado com o intuito de torná-lo mais explícito. Quanto à metodologia fez-se a opção pelo método dedutivo. Esta opção se justifica porque o método escolhido permite uma análise aprofundada acerca do tema. Em relação ao procedimento optou-se por uma abordagem direta. E por fim, utilizar-se-á de pesquisas bibliográficas, com análises de livros, artigos e outros meios impressos e eletrônicos relacionados ao assunto.

1.6 ESTRUTURA DO TRABALHO

No primeiro capítulo apresentamos a introdução com a contextualização do estudo; formulação do problema de pesquisa; as proposições do estudo; os objetivos geral e específico; as justificativas, relevância e contribuições da proposta de estudo; a metodologia do estudo, bem como definição estrutural da monografia.

No segundo capítulo discorremos sobre como é feita a prevenção e o combate estatal em relação aos crimes eletrônicos, a evolução histórica, e conceituação dos crimes cibernéticos.

No terceiro capítulo, serão apresentadas as classificações deste meio de delito, assim como suas modalidades e seus tipos, além de arrazoar as grandes redes utilizadas para a prática dos atos ilícitos, e como de fato ocorre um crime virtual.

Por fim, no quarto capítulo analisamos a legislação vigente e projetos de leis acerca dos crimes virtuais.

2. CIBERCRIMES E ATUAÇAO ESTATAL

2.1 EVOLUÇÃO HISTÓRICA

Na década de 1970, surgiu nos Estados Unidos a internet, enquanto o Departamento de Defesa Norte-Americano criou um método que estabelecia conexão vários centros de pesquisas militares, autorizando a entrega de informações e dados. Só ao acúmulo foi realizável devido a quantidade de estudos sobre a informática, e igualmente ao crescimento dos computadores (TEIXEIRA, 2007).

No início, o seu uso na época estava limitado apenas aos Estados Unidos, para fins de pesquisas em universidades, mais tarde se expandiu ao uso comercial e depois, se ampliou ao continente Europeu. A rede foi ganhando dimensão nas realidades sociais, e na década de 80, evolui para o termo internet. O tempo, e as pesquisas realizadas foram elementos cruciais para o que hoje possível, por meios tão rápidos e simples (TEIXEIRA, 2007).

O surgimento dessa nova tecnologia possibilitou ao ser humano várias mudanças e conceitos, englobando todas as áreas de qualquer usuário, seja no ramo profissional, proporcionando o rápido movimentação de envios de dados, ou no lazer, contribuindo para o colhimento de notícias de todo o mundo em muito pouco tempo, com o acesso a jornais e revistas online, por exemplo. Com todo esse mecanismo, quem poderia delinear que algo feito com o intuito justo, fosse atingir proporções tão criminosas como as que hoje são percebidas? Assim como todas as coisas disponíveis ao ser humano se tornam objeto de crueldade em algum momento, com a internet não poderia ser diferente (LIMA E DUARTE, 2020)

Apesar do conceito ser antigo, a citação “cibercrime” surgiu somente no final da década de 90, em uma reunião que se destinava à um debate sobre o combate as práticas ilícitas na internet com punições e medidas que visam coibir esses atos. Desde então, o termo passou a ser usado para designar infrações penais praticadas online. (D’URSO, 2017)

No entanto, a sucessiva mutação tecnológica dificulta o combate aos delitos, que estão simultaneamente crescendo com as novas tecnologias. Assim, com o uso

incontido e indiscriminado da web, alguns indivíduos com conhecimento em informática passaram a se aprimorar e utilizar esses conhecimentos roubando informações criptografadas, como já havia acontecendo há tempos, para obter proveito econômico ou ainda, por mera diversão. Sujeitos esses que ganharam a pronunciação de hackers, um indicativo atual para sujeitos que sempre existiram. Portanto, com o desenvolvimento e popularização da internet, a quebra de códigos e invasão de sistemas deixou de ser um instrumento de guerras para se tornar uma oportunidade de lucro ilícito ou mero passatempo, fazendo da criminalidade virtual uma doença social. (JESUS e MILAGRE, 2016)

2.2 ASPECTOS CONCEITUAIS DOS CRIMES CIBERNÉTICOS

Variadas são as denominações para o tipo penal, alguns autores de forma brevemente descrevem os cibercrimes (INTERPOL, 2015) como atividade criminosa ligada diretamente a qualquer ação ou prática ilícita na Internet. Consistindo o crime em fraudar a segurança de computadores, sistema de comunicação e redes corporativas. Assim, o cibercrime, nada mais é do que uma conduta ilegal realizada por meio do uso do computador e da internet (ROSA, 2002, p.53-57).

No entanto, esses delitos possuem um significado bastante complexo, podendo alcançar tanto um único usuário, quanto grandes empresas, órgãos públicos e organizações. Além disso, por se tratar de um instrumento eficiente, esses criminosos possuem a facilidade, de ao mesmo tempo, fazer diferentes vítimas em ataques variados e em lugares diversos. (UPIS, 2019)

Outros autores como Frabízio Rosa, (2006, p. 55), conceitua de uma forma mais expressiva e detalhada os crimes virtuais, apresentando que:

> A ação atente contra o estado natural dos dados e recursos oferecidos por um sistema de sequência de dados, seja pela compilação, armazenamento ou entrega 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; 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; Assim, o “Crime de Informática" pressupõe dois 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; A expressão crimes de informática, entendida como tal, é toda

> a ação típica, antijurídica e culpável; 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.

Decerto se tem todos os tipos de condutas delituosas que são praticadas online, desde pedofilia, prostituição, tráfico, pirataria, até sabotagem e terrorismo. A digitalização dos métodos de trabalho tem causado ao Brasil, transtornos provocados por uma nova onda de crimes cibernéticos.

No Brasil, por exemplo, o Hospital do Câncer de Barretos, e outros administrados pela Fundação Pio XII, tiveram as fichas de seus pacientes sequestradas e o resgate pedido era de quase mil reais por computador em bitcoins (dinheiro virtual). O mesmo ficou com seu sistema desativado por três dias, o que gerou atrasos e prejuízos a muitos pacientes. (VEJA, 2017)

Muito se sabe o quanto tem crescido as modalidades para praticar esses delitos, nosso país já tem em sua história condutas informáticas danosas. Outro exemplo dessa infeliz estatística é o do ex-prefeito Paulo Maluf, o qual, nas eleições de 2003, foi o primeiro político a sofrer sabotagem digital. Os hackers invadiram o site do político espalhou e-mails a todos os eleitores cadastrados, divulgando mensagens de cunho difamatório. (SOARES, 2000)

2.3 A PREVENÇÃO E O COMBATE DO ESTADO AOS CIBERCRIMES

Diante da emergência de saúde pública ocasionada pela pandemia do coronavírus, a ocorrência de crimes cibernéticos tomou proporções ainda maiores. A medida de prevenção de isolamento social fez com que os 134 milhões de usuários de Internet brasileiros passassem a depender ainda mais da internet e das Tecnologias de Informação e Comunicação (TICs), para realizar atividades como o trabalho remoto, ensino a distância, compras virtuais, telemedicina e até mesmo para acessar o auxílio emergencial conferido pelo governo, criando ambiente fértil para a propagação de vários ataques cibernéticos.(FERREIRA, SERRAGLIO, CANHOTO, ARAGÃO, CHICARONI, 2020)

Esses crimes virtuais só tem o internauta como vítima se ele não for previamente instruído sobre essas agressões, já que esse tipo de ato ilícito é um dos únicos que a vítima sai com êxito ao reagir à agressão. Em consequência disso, um dos órgãos que vem se destacando na buscar para melhor proteger e instruir a sociedade é o Ministério Público do Estado da Bahia que criou um núcleo específico para atender a demanda dos atos ilícitos virtuais, esclarecer as dúvidas da população e contribuir no combate a esses delitos com o Núcleo de Combate aos Crimes Cibernéticos (NUCCIBER).

> Com a finalidade de articular, em conjunto com os Promotores de Justiça, medidas judiciais e extrajudiciais necessárias à efetivação do combate aos crimes cibernéticos de competência e âmbito estadual, o Núcleo de Combate aos Crimes Cibernéticos do Ministério Público do Estado da Bahia – NUCCIBER – fornece todo o suporte basilar que fundamente tais medidas ou que possibilite a identificação da autoria delitiva para prosseguimento em investigações tradicionais. À denúncia de crime cibernético pode ser efetuada em qualquer canal de acesso ao cidadão, a saber, pessoalmente, por telefone, site ou e-mail. Ao receber a denúncia de um crime virtual em um dos departamentos da Instituição, esta será encaminhada ao Promotor de Justiça competente para atuar e dar andamento a solução desta demanda. Havendo a flagrante necessidade de atuação, o Núcleo de Combate aos Crimes Cibernéticos do Ministério Público do Estado da Bahia – NUCCIBER – é acionado para prestar auxílio. A partir do recebimento de ofício requerendo investiga- 63 ções preliminares, o Núcleo diligência a situação. (PATURY, SALGADO, TEIXEIRA FILHO. 2017. Pág. 10).

Pode-se observar que preliminarmente a investigação se inicia por meio de artifícios disponibilizados na web no qual se retira todas as informações pertinentes a respeito do caso em questão com o intuito de encontrar o dispositivo informático percussor do ato ilícito.

É apresentado muitas medidas preventivas fomentando a devida instrução legal da população em conformidade com a Lei 12.965/14, estabelecendo assim a inclusão digital mais segura da população, fomentando uma navegação na web mais ética (NUCCIBER)

É necessário, para um melhor combate contra os crimes cibernéticos, a capacitação e treinamento dos membros do Poder Judiciário sobre os perigos que a internet reserva, cursos sobre as redes sociais e suas possíveis manipulações indevidas como também as particularidades dos crimes digitais, os conceitos sobre esse novo perigo eminente, o respaldo na sociedade, os novos bens jurídicos

emergentes, juntamente com as possíveis formas de investigação. (PATURY, SALGADO, TEIXEIRA FILHO, 2017)

> Em um primeiro momento a oficina versa sobre Introdução à Crimes Cibernéticos. Neste encontro é repassada a parte conceitual desta nova modalidade de delito, ressaltando as formas de configuração de um Crime Cibernético e suas classificações. Importante também é reforçar os termos técnicos da área de Tecnologia da Informação mais usuais e de grande valia para fomentar o diálogo entre os órgãos investigativos. Na explanação seguinte, os profissionais desenvolvem as noções preliminares da prática investigativa. Casos concretos de investigação como cyberbulling, fraudes eletrônicas e bancárias, práticas de phishing Scam, crimes cometidos através de emails, pedofilia, racismo, dentre outros são apresentados, debatidos e trabalhados nas oficinas. (PATURY, SALGADO, TEIXEIRA FILHO. 2017. Pág. 13).

Assim também, instruindo os profissionais sobre a preservação da privacidade, a maneira correta de se executar a liberdade de expressão na web sem ferir a ética, a responsabilização pelos conteúdos publicados em suas redes sociais como também o respaldo das mesmas, tudo isso vislumbrando o combate a inércia estatal em face aos delitos virtuais. (PATURY, SALGADO, TEIXEIRA FILHO, 2017)

Outra forma de prevenção seria através da realização de palestras educativas nas escolas e universidades, que possam ensinar como melhor usar a internet, evitando a exposição desnecessária dos usuários. Alertando sobre o uso moderado da internet para uma melhor vida saudável e social. Pois o jovem que compartilha algo na web está lançando uma informação sua a todo o público mundial e o Estado deve conscientizar a população de que após se publicar algo na internet se perde o controle dessa publicação, já que quando ela é disponibilizada no mundo virtual permite-se que qualquer pessoa a veja ou faça download. (PATURY, SALGADO, TEIXEIRA FILHO, 2017)

Outro perigo emergente na web são os fakes, que se tratam de pessoas que criam uma espécie de personagem para poder obter vantagens sobre outras extraindo informações ou as persuadindo a prática de algum ato. Desse modo, não existe uma barreira de proteção adequada para os usuários (PATURY, SALGADO, TEIXEIRA FILHO, 2017).

Ainda mais interessante e necessário seria a criação de uma nova lei, pois, o Brasil ainda não foi contemplado com uma legislação específica que regulamente todas as hipóteses pertinentes aos crimes cibernéticos, por isso deixa a sociedade desprotegida nesse aspecto. Assim, é necessário o estudo e uma análise minuciosa de uma possível redação legal que possa regulamentar as condições e políticas que devem ser adotadas na web, a tipificação de condutas danosas ou reprováveis pela sociedade, os crimes cibernéticos e também as devidas punições, a regulamentação dos provedores, bem como das plataformas dos sistemas, a criminalização da propagação de vírus e qualquer outra conduta ou artifício referente a seara digital que respalde negativamente no âmbito social ou fira a dignidade da pessoa humana. O ordenamento jurídico brasileiro precisa de uma regulamentação específica que possa proteger os novos bens jurídicos que emergiram da tecnologia (PATURY, SALGADO, TEIXEIRA FILHO, 2017).

3. TIPOS PENAIS, DESDOBRAMENTOS DA PRÁTICA DESTE CRIME

3.1 SUAS CLASSIFICAÇÕES E MODALIDADES

Atualmente, cresce o número de pessoas que acessam a internet. Existem diversos websites na rede mundial de computares e a cada dia são criadas mais de mil homepages. Na internet atual é possível se encontrar basicamente de tudo desde comprar um livro até mesmo participar de uma graduação a distância, o que ocorre é que todo usuário que deste meio usufrui estão expostos aos mais variados crimes pois não há barreiras concretas para que estes deixem de perpetuar por toda rede causando imensos estragos no cotidiano dos internautas de boa-fé. (MARTINS, 2017)

Constatar e classificar um crime virtual não é tarefa simples e fácil, pois ainda são poucas as conclusões existentes. O fato se deve a tecnologia, que evolui rapidamente e a opinião dos legisladores segue no mesmo ritmo. Alguns criminosos utilizam computadores para cometer de crimes, porém há casos que sem a informática não seria lógico o cometimento de determinados crimes. Neste sentido Crespo (2011, p.60) referenciando a Tiedemann que formulou em 1980 as classes dos delitos de informática:

> a) Manipulações: podem afetar o input (entrada), o output (saída) ou mesmo o processamento de dados; b) Espionagem: subtração de informações arquivadas abarcando-se, ainda, o furto ou emprego indevido de software; c) Sabotagem: destruição total ou parcial de programas; d) Furto de tempo: utilização indevida de instalações de computadores por empregados desleais ou estranhos.

GRECO FILHO (2000, p.85) fraciona as classes da seguinte forma tendo em vista condutas contra sistemas de informática e condutas contra outros bens jurídicos:

> Focalizando-se a Internet, há dois pontos de vista a considerar: crimes ou ações que merecem incriminação praticados por meio da internet e crimes ou ações que merecem incriminação praticados contra a Internet, enquanto bem jurídico autônomo. Quanto ao primeiro, cabe observar que os tipos penais, 15 no que concerne à sua estrutura, podem ser crimes de resultado de conduta livre, crimes de resultado de conduta vinculada, crimes de mera conduta ou formais (sem querer discutir se existe distinção entre estes) e

> crimes de conduta com fim específico, sem prejuízo da inclusão eventual de elementos normativos. Nos crimes de resultado de conduta livre, à lei importa apenas o evento modificador da natureza, com, por exemplo, o homicídio. O crime, no caso, é provocador o resultado morte, qualquer que tenha sido o meio ou a ação que o causou.

Existem distinções em todas classificações expostas contudo há também pontos em comum, alguns posicionamentos têm como objeto protegido os meios eletrônicos, ou seja, o bem jurídico e outras como o meio eletrônico com forma ou instrumento de lesionar outros bens jurídicos tornando esta última um entendimento que abarca mais acerca das práticas. (MARTINS, 2017)

Vários autores usam o termo “crime” quando falam de condutas lesivas a sistemas informáticos, a dados ou informações. Assim, verificar condutas criminosas que se propagam pela internet é uma tarefa delicada, pois é difícil localizar onde o agente que efetuou o crime se encontra, pois, a prática destes delitos não encontra barreiras pela internet e circulam livres pelo sistema global de comunicação mundial. (MARTINS, 2017)

A maioria destas ações delituosas ocorrem tanto pela rede quanto pelo mundo real, porém alguns crimes têm certas peculiaridades o que torna necessário uma adequação quanto ao seu tipo penal. Deste modo, analisamos a seguir algumas modalidades de crimes cibernéticos. (MARTINS, 2017)

3.1.1 INVASÃO E PRIVACIDADE

Pela atuação da grande parte da população utilizando a rede mundial de computadores, iniciou a ramificar de forma bem ampla um número ilimitado de informações nesta rede, tanto informações que são inseridas através de cadastro em sites comerciais, quanto preenchimento de formulários eletrônicos para através de perfis para adesão a redes sociais. (DIWAN, 2016)

Os usuários utilizam as redes para acesso a diversos tipos de dados, pois a internet possibilita a realização de várias atividades, o que ocorre é que todas informações disponibilizadas com ou sem autorização pela internet, podem trazer

penalidades a pessoas jurídicas ou físicas que usam destas informações sem consentimento. (DIWAN, 2016)

O código civil brasileiro também garante a proteção da privacidade, assim como também a Constituição Federal (CF), quem em seu artigo 5º, X, garante a qualquer cidadão que não tenha a sua privacidade respeitada, o direito a reparação, sendo aquela considerada inviolável.

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a 17 inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: 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;

O que se deve é resguardar o cidadão também no que diz respeito aos seus dados disponibilizados na internet, sejam eles inseridos através de órgãos públicos, comercio eletrônico ou até mesmo através de entes privados. Informações pessoais de qualquer pessoa natural ou jurídica não deveriam ser tratadas como mercadorias desconsiderando assim seus aspectos objetivos. Ë dever do Estado garantir ao cidadão o direito de proteção a sua identidade, e que dados disponibilizados sejam usados somente para um objetivo específico. (SILVA, 2020)

3.1.2 ESPIONAGEM ELETRÔNICA

Atualmente, a utilização de tecnologias da informática por pessoas é crescente, com isso também cresce a dependência das empresas por softwares diversos, o que eleva o tempo de conexão de ambas situações a rede mundial de computadores, ocasionando o lançamento elevado de informações estratégicas e pessoais nos servidores empresariais. Essa prática aumenta a necessidade de prevenção e monitoramento da segurança da informação. O Código Penal não tipifica de forma específica o crime de espionagem eletrônica, sendo que a conduta este definida no Código Penal em seus artigos 154 e 154ª

> Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem: Pena – detenção, de três meses a um ano, ou multa. Invadir

> dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena – detenção, de três meses a um ano, ou multa.

A CLT versa em seu artigo 482, “g” que o funcionário que o funcionário que praticar a conduta poderá ter seu contrato rescindido “Constituem justa causa para rescisão do contrato de trabalho pelo empregador: g) violação de segredo da empresa”. Patrícia Peck (2010, p. 385) nos diz que:

> É primordial a aplicação de medidas em três níveis, físico, lógico e comportamental para o combate a espionagem, alguns pontos devem ser observados tais como controles mais rígidos dos insider; Frequência e controle de acesso em conjunto com a máquina; Uso de softwares de monitoramento; regulamentação de equipamentos moveis e bloqueio de portas USB; Criação de canal de denúncia; Garantia de acesso somente a que é necessário; realização de testes de vulnerabilidade.

Em ambiente laboral, deve-se haver mais segurança através de investimentos por parte das empresas, tendo em vista que ameaças internas são mais difíceis de serem rapidamente identificadas, pois o agente que exerce tal conduta é um usuário considerado legítimo evitando seu rastreamento (MARTINS, 2017).

3.1.3 FRAUDES VIRTUAIS

A internet moderna proporciona aos seus usuários a interação em tempo real, ferramentas com e-mail e chat que são constantemente utilizados de forma pratica e rápida por todos usuário da rede. Da mesma forma, a navegação web e os games podem proporcionar lazer e acesso à educação de forma interativa. Em crimes definidos como Fraude Virtual, a conduta aplicada é a de invasão, modificação ou alteração, adulteração em sistema de processamento de dados ou supressão de dados eletrônicos ou programa (SILVA, 2019).

O CERT-BR (Centro de estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil) diz que fraude eletrônica se dá por: “Mensagem não solicitada afim de se passar por instituição conhecida ou ainda a mensagens que induzem o usuário a instalar de códigos de origem duvidosa”. (Disponível em https://www.cert.br/, acessado em 16 de maio de 2021).

Fraudes virtuais possuem duas modalidades: As fraudes externas, onde quem comete a fraude não tem vínculo direto com o local a ser fraudado e a fraude interna que é cometida por aquele infrator que está dentro do local a ser fraudado seja ele um morador ou empregado ou mesmo um terceiro que esteja prestando serviço ou de passagem pelo local (MARTINS, 2017).

Na prática dos crimes envolvendo fraudes virtuais, o usuário é induzido a fornecer seus dados financeiros ou pessoais. Parte das ações atualmente praticadas, os fraudadores tentam através das redes sociais maneiras de convencer usuários a fornecer dados pessoais (MARTINS, 2017).

3.1.4 CRIMES CONTRA A HONRA

Qualidades físicas, morais e intelectuais de um indivíduo são a sua honra. A honra deve ser protegida pois é um patrimônio que a pessoa possui, sendo ela subjetiva, constituída por sentimentos próprios de respeito, de moral, de atributos intelectuais entre outros. Crimes contra a honra estão previstos no código penal brasileiro e estes são os crimes mais comuns cometidos através da internet. O crime de difamação é um dos crimes contra a honra, este está definido no artigo 139 do código penal:

> Difamar alguém, imputando-lhe fato ofensivo à sua reputação: Pena – Detenção, de 3 (três) meses a 1 (um) ano, e multa.

Difamar é um tipo de crime que ataca a honra objetiva da pessoa, este crime é praticado na internet em diferentes formas tanto imputando ao indivíduo algum fato que ofenda sua honra objetiva através de e-mail ou até mesmo publicando ofensas em redes sociais.

No artigo 139 do código penal, a norma é destinada a pessoa humana, logo o crime de difamação a pessoa jurídica não pode ser sujeito passivo, neste caso pode se aplicar a lei nº 5.250/67 – Lei de Imprensa INELLAS (2004, p.51).

Diferente do crime de calúnia no art. 138 do Código Penal Brasileiro, o Crime de difamação não exige que a atribuição seja falsa bastando somente o agente sentir sua honra ofendida perante a sociedade e o crime se consuma no momento

em que o terceiro toma conhecimento do fato, já em ambiente virtual o crime irá se consumar, por exemplo, quando houver a propagação do ato ofensivo através das redes sociais. (LOPES, 2017)

O Crime de Calúnia está descrito no art. 138 do Código Penal, o qual versa:

> Caluniar alguém, imputando-lhe falsamente fato definido como crime. Pena – Detenção de 6 (seis) meses a 2 (dois) anos, e multa.

No crime de Calúnia o agente imputa a alguém um crime e abala sua reputação frente a sociedade abalando assim sua honra objetiva. Já o crime de injúria, que está previsto no artigo 140 do código penal, o agente propaga de forma negativa uma qualidade da vítima, qualidade esta que diga respeito aos seus atributos morais, físicos ou intelectuais ofendendo de forma subjetiva a hora da vítima (MARTINS, 2017).

3.1.5 PORNOGRAFIA INFANTIL

Pedofilia é um ato de perversão que leva um indivíduo já em fase de vida adulta a se sentir sexualmente atraído por crianças ou mesmo a prática de atos sexuais com estas. A pedofilia há anos aflige o mundo, mas com a popularização da internet ficou mais em evidência, levando ser mais estudada e analisada no âmbito jurídico e psicológico. Apesar de ser causa de repúdio por boa parte da sociedade, infelizmente, há na internet diversas figuras com este tipo de material. O código penal, em seu artigo 234, versa:

> Fazer, importar, exportar, adquirir ou ter sob sua guarda, para fim de comércio, de distribuição ou de exposição pública, escrito, desenho, pintura, estampa ou qualquer objeto obsceno: Pena – detenção, de 6 (seis) meses a 2 (dois) anos, ou multa. Parágrafo único. Incorre na mesma pena quem: I – vende, distribui ou expõe à venda ou ao público qualquer dos objetos referidos neste artigo; II – realiza, em lugar público ou acessível ao público, representação teatral, ou exibição cinematográfica de caráter obsceno, ou qualquer outro espetáculo, que tenha o mesmo caráter; III – realiza, em lugar público ou acessível ao público, ou pelo rádio, audição ou recitação de caráter obsceno.

O elemento subjetivo aqui é o dolo, pois o infrator tem o objetivo de comercializar o objeto material do crime ou mostrar ao público, a disponibilização do material ou possibilidade de alguém ter acesso ao mesmo já configura a pratica deste delito. Na Pedofilia existe uma perversão sexual pois o adulto se relaciona de forma erótica com crianças ou adolescentes, já na Pornografia infantil não é necessário que haja relacionamento, bastando somente a divulgação ou comercialização de material erótico envolvendo crianças ou adolescentes. (SILVA, 2019)

A lei 8.069/90, O Estatuto da Criança e do Adolescente, tipifica esse tipo penal em seu artigo 241, II sendo considerado crime a divulgação/publicação de imagem contendo material pornográfico de crianças ou adolescente, estabelecendo penalidades ao pedófilo e todo aquele que comercializa material de pornografia infantil. O ECA assim versa:

> Art. 240 – Produzir ou dirigir representação teatral, televisiva ou película cinematográfica, utilizando-se de criança ou adolescente em cena de sexo explícito ou pornográfica: Pena – reclusão de 1 (um) a 4 (quatro) anos, e multa. Parágrafo único. Incorre na mesma pena que, nas condições referidas neste artigo, contracena com criança ou adolescente. Art. 241 – Fotografar ou publicar cena e sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão de 1 (um) a 4 (quatro) anos.

O Supremo Tribunal Federal entende que basta a divulgação e o crime já está consumado independente do meio utilizado. Entendimento da Colenda da Primeira turma do STF:

> ESTATUTO DA CRIANÇA E DO ADOLESCENTE – Art. 241 – Inserção de cenas de sexo explícito em rede de computadores (Internet) – Crime caracterizado – Prova pericial necessária para apuração da autoria. “Crime de computador”; publicação de cena de sexo infanto-juvenil (E.C.A., art. 241), mediante inserção em rede BBS/Internet de computadores atribuída a menores – Tipicidade – Prova pericial necessária à demonstração da autoria – Habeas Corpus deferido em parte.
> O tipo cogitado – na modalidade de “publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente” – ao contrário do que sucede por exemplo aos da Lei de Imprensa, no tocante ao processo da publicação incriminada é uma normal aberta: basta-lhe à realização do núcleo da ação punível a idoneidade técnica do veículo utilizado à difusão da imagem para número indeterminado de pessoas, que parece indiscutível na inserção de fotos obscenas em rede BBS/Internet de computador. 2. Não se trata no caso, pois, de colmatar lacuna da lei incriminadora por analogia: uma vez que se compreenda na decisão típica da conduta incriminada, o meio técnico empregado para realizá-la pode até ser de invenção posterior

> à edição da Lei penal: a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada a outrem mediante arma de fogo. 3. Se a solução da controvérsia de fato sobre a autoria da inserção incriminada do conhecimento do homem comum, impõe se a realização de prova pericial.

Muitas vezes, uma perícia técnica rigorosa deve analisar as provas eletrônicas para que essas sejam aceitas em processo. Contudo conclui-se que a exposição de uma criança ou adolescente de forma pornográfica na internet tem como pena a reclusão de 2 a 6 anos e multa. (SILVA, 2019)

3.1.6 ESTELIONATO

O estelionato é uma das práticas de crime mais popular do nosso ordenamento jurídico, o número de pessoas que tentam adquirir para si ou para outro vantagens ilícitas, aumenta tanto com o uso da internet quanto fora dela. As condutas variam conforme os meios eletrônicos disponíveis. O código penal em seu artigo 171 assevera que:

> Art. 171. 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: Pena – reclusão, de 1 (um) a 5 (cinco) anos, e multa.

Pela internet é comum um estelionatário utilizar condutas típicas tal com encaminhar para um usuário qualquer um e-mail com conteúdo falso fazendo o destinatário acreditar que ao acessar o link enviado no corpo deste e-mail o mesmo será direcionado para um site confiável afim de atualizar seus dados cadastrais, tendo assim o criminoso formas de adquirir informações pessoais ou confidenciais daquele usuário. Na maioria das vezes essa prática ocorre para apropriação de dados bancários.

Existem formas na rede mundial de computadores de tentar se livrar destes e-mails indesejados, uma destas formas seria a atualização de sistemas de proteção como Firewall e Antivírus, o qual servirão de barreiras para potenciais intrusos controlando, assim, as regras de transferência de documentos. (TORMEN, 2018)

4. LEGISLAÇÃO CORRESPONDENTE

4.1 LEI DOS CRIMES CIBERNÉTICOS (LEI Nº 12.737/12)

O elevado crescimento no número de crimes virtuais e sua influência na sociedade levaram o legislador a elaborar normas jurídicas que visam coibir tais condutas. A primeira delas, criada exclusivamente para a tipificação de crimes virtuais, é a Lei dos Crimes Cibernéticos (Lei nº12.737/12) ou, como é mais conhecida, Lei Carolina Dieckmann, a qual foi publicada no Diário Oficial da União e sancionada pela ex-Presidenta da República, Dilma Rousseff em 2 de dezembro de 2012. Este marco representou um grande avanço no nosso ordenamento jurídico no que se refere ao combate dos crimes virtuais. (SANTOS, 2020)

Essa lei objetiva tipificar condutas altamente gravosas como invasão de computadores, roubo de senhas, violação de dados dos usuários e divulgação de informações privadas (como fotos, vídeos e mensagens). Já havia sendo postulado diante do grande volume de golpes e roubos de senhas pela internet, porém, antes mesmo de publicada e sancionada, ganhou notoriedade na mídia com o caso da atriz Carolina Dieckmann. O fato se deu em maio de 2012, situação na qual a atriz global teve seu computador invadido e seus arquivos pessoais subtraídos, inclusive com a publicação de 36 fotos íntimas que rapidamente se espalharam pela internet através das redes sociais. (VITORIANO, 2018).

O hacker exigiu dez mil reais da atriz para que não publicasse as fotos, porém, Carolina foi à polícia imediatamente e realizou a denúncia. Em razão desse episódio, a atriz, por 26 ser mulher com grande influência, abraçou a causa e acabou cedendo seu nome para vinculação à nova lei. Devido a esse acontecido e por pressão da mídia e da população, reacendeu novamente o debate acerca dos crimes cibernéticos, gerando um momento propício para a aprovação desta lei. Por esse motivo a mesma foi votada e sancionada rapidamente. (QUINTINO, 2012)

O universo jurídico precisou incluir no Código Penal os crimes cometidos no ambiente virtual. Com a alteração, o referido código recebeu o acréscimo dos artigos 154-A e 154- B no Capítulo VI, que trata dos crimes contra a liberdade individual,

mais precisamente na seção dos crimes contra a inviolabilidade dos segredos. (QUINTINO, 2012)

O artigo 154-A estabelece a importância de incriminar o agente que dribla os mecanismos de segurança, invadindo, adulterando ou destruindo a privacidade alheia, com a finalidade de adquirir vantagem ilícita. Entretanto, esse dispositivo exige a necessidade de que o mecanismo de segurança desse aparelho seja violado indevidamente, definindo, portanto, como fato atípico se inexistente tal mecanismo de segurança (QUINTINO, 2012). Assim temos, segundo o artigo 154-A, que:

> Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita recebe pena de detenção de 3 meses a 1 ano, e multa.

Aumenta-se a pena, caso o crime seja cometido contra chefes de Estado, conforme artigo acima, inciso § 5º:

> I – Presidente da República, governadores e prefeitos; II – Presidente do Supremo Tribunal Federal; III – Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou IV – dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Enquanto isso o art.154-B prevê que:

> Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

Os crimes considerados menos gravosos, como os estabelecidos no artigo 154-A como “invasão de dispositivo informático”, são punidos com prisão de três meses a um ano e multa. Por outro lado, as condutas mais danosas, como obter, pela invasão, conteúdo de “comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas” podem ter pena de seis meses a dois anos de prisão, além de multa. (SANTOS, 2020)

A alteração do Código Penal brasileiro em razão da lei referida trouxe os artigos 266 e 298 que na realidade não representam propriamente uma inovação, pois já eram condutas previstas pela legislação brasileira, apresentando como novidade somente algo mais concreto. O que se pretendeu foi integrar ao texto normativo, condutas que antes não geravam penalidade alguma, em razão da inexistência de tipificação específica. (WANDERLEY, P.44, 2014).

O artigo 266, anteriormente citava os serviços radiotelegráficos em seu caput, o que com o tempo, se encontrou em desuso. A partir disso, com o intuito de trazer ao dispositivo uma maior atualização sobre os meios comuns de comunicação e transmissão de dados, o legislador acabou acrescentando em seu §1, para fim de punição, o serviço telemático, bem como o serviço de informação de utilidade pública para quem os interrompe ou dificulta seu restabelecimento (WANDERLEY, P.44, 2014). Assim temos que:

> Artigo 266 – Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento. §1 Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

A pena para esses crimes é de detenção, de um a três anos e multa. Além disso, seu §2 menciona a aplicação em dobro da pena se o crime for cometido por ocasião de calamidade pública. Sobre o artigo 298, foi acrescentado a ele o parágrafo único, isso porque, o legislador preferiu alterar o tipo falsificação de documento particular e gerou indiscutível tipicidade nas condutas modernas de modificação ou fabricação de cartões, satisfazendo os interesses dos particulares lesados e dos bancos violados. (SYDOW, 2000)

Diante disso, a inclusão da equiparação de cartão de crédito ou débito como documento particular, não gera a menor dúvida sobre responsabilização penal nos casos de 28 clonagens de cartões, falsificação de numeração, entre outras alterações. (ANANIAS; WANDERLEY, P.45, 2014).

> Artigo 298 – Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro: Pena – reclusão, de um a cinco anos, e multa. Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.

Muitos especialistas e juristas criticam a lei mencionada em razão de sua amplitude e não especificação do meio em que é cometido o crime, por exemplo. Além disso, também há diversas interpretações em relação à abrangência do enquadramento e a fiscalização dos crimes. Afinal, combater os crimes cibernéticos no país ainda é muito desafiador por conta da dificuldade no rastreio das informações. (SANTOS, 2020)

Por esse motivo se é dito que o texto normativo em questão, o qual tinha como finalidade promover mudanças, não produziu, na realidade, grandes reformas no nosso ordenamento jurídico, nem ao menos resolveu o problema enfrentado pelo Direito brasileiro sobre o assunto. Diante disso, se entendeu necessária a criação de uma nova lei que estabeleceria aos usuários e provedores de internet segurança e direito individual. Essa lei foi nomeada de Lei do Marco Civil da internet (Lei nº 12.965/14). (SANTOS, 2020)

4.2 MARCO CIVIL DA INTERNET (LEI Nº12.965/14)

O ambiente online se torna, cada dia mais, um terreno aberto aos delitos virtuais. Engana-se quem pensa que o mundo online é uma terra sem leis. Por esse motivo, desde 2014, o espaço cibernético é regido pelo Marco Civil da Internet, que estabelece direitos e deveres aos internautas. A Lei nº 12.965/14, aprovada na Câmara dos Deputados em 25 de março de 2014 e no Senado Federal em 23 de abril de 2014, ou apenas Marco Civil da Internet, foi regulamentada com a finalidade, segundo a advogada Morgana Alencar (2019), bacharel em Direito pela UFMA e pós graduada em Direito do Trabalho e Previdenciário pela PUC – Minas, de estabelecer princípios, garantias, direitos e deveres para o uso da internet no Brasil, bem como regular como se daria nesse contexto a atuação da União, dos Estados, do Distrito Federal e dos Municípios. A mencionada lei atentou-se em estabelecer a forma 29

como os direitos, sendo eles constitucionais ou não, permaneceriam sendo protegidos no ambiente virtual. (ALENCAR, 2019)

Em vigor desde 23 de junho de 2014, antes mesmo de virar lei, os conteúdos citados por ela foram elaborados com participação da população por meio de apresentação em debates e audiências públicas em todo o Brasil. Época em que já era possível opinar e comentar os artigos também pelo blog Cultura Digital e pelos portais e-Democracia e e-Cidadania, da Câmara dos Deputados e do Senado Federal. (MEYER, 2018)

O Marco Civil da internet se deu pela necessidade do nosso ordenamento se ajustar à evolução da sociedade promovida pela tecnologia visto que anteriormente acreditava-se que a internet seria uma “terra sem lei” e não passível de regulamentação, considerando que as informações circulavam por ela de forma descontrolada e sem fiscalização adequada. Nesse sentido, a normatização passou a ser essencial a partir do momento em que se verificou que as relações construídas na internet impactavam vidas além do mundo virtual. Vale ressaltar que as normas devem ser submetidas também às empresas internacionais, que operam em território brasileiro. (SANTOS, 2020)

A referida lei foi sancionada pela ex-Presidenta Dilma Rousseff com certa urgência, devido a descoberta de espionagem do governo americano, mediante meio eletrônico, sobre dados tanto do governo brasileiro quanto de algumas empresas também brasileiras, justificados como uma forma de segurança. Já a advogada Tayrine Queiroz (2015) sinaliza que:

> Muitos alegavam ser um projeto ainda deficiente, sendo necessária a supressão de algumas falhas e que a urgência em aprovar tal projeto respaldava-se numa tentativa de autopromoção do governo brasileiro, para que a presidenta pudesse apresentar a lei na conferência da NETmundial, que ocorreria em São Paulo, onde representantes de todo o mundo discutiriam sobre meios de regulamentar a Internet.

A Lei nº12.965/14 possui 32 artigos divididos em 5 capítulos, os quais tratam principalmente dos princípios da privacidade, da neutralidade e da guarda de registros de acesso, com o fim de regular o uso da internet no Brasil. A referida lei determina ainda limitações a respeito do armazenamento de informações pessoais

dos usuários ao exigir que só será possível se respeitadas determinadas garantias. (SANTOS, 2020)

Inicialmente são previstos por ela os fundamentos e princípios que devem ser observados no uso da internet, dispondo, por exemplo, sobre garantias como a liberdade de expressão, defesa do consumidor e proteção da liberdade e da privacidade. Assim, a partir da publicação do Marco Civil da internet, foi disponibilizada aos usuários uma maior segurança aos seus dados pessoais com o intuito de impedir que terceiros se utilizassem indevidamente dessas informações armazenadas. O artigo 7º vem para assegurar este direito através da anuência expressa do usuário, além da proteção da intimidade e da inviolabilidade da vida deste.

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I – inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; II – não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei." [...] VIII- Informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet.

O princípio da privacidade (artigo 11º da lei mencionada) diz respeito à garantia da inviolabilidade, da confidencialidade e do sigilo das relações virtuais dos usuários. Com isso, a lei prevê somente exceção mediante ordem judicial nos casos em que estas informações possam contribuir na investigação.

> Artigo 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em 31 território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

Ademais, encontra-se no artigo 12 desta lei a previsão de sanções, caso haja descumprimento de qualquer termo supramencionado, sem interferir na imposição das demais penalidades criminais ou administrativas. Assim temos que:

> Artigo 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts.10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa: I - Advertência, com indicação de prazo para adoção de medidas corretivas; II - Multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção; III - Suspensão temporária das atividades que envolvam os atos previstos no art.11; ou IV - Proibição de exercício das atividades que envolvam os atos previstos no art.11.

Tal como a lei tratada anteriormente, apesar da Lei nº 12.965/14 ter contribuído com importantes inovações para era digital, tal feito não foi suficiente para assegurar completamente os dados pessoais dos usuários devido a insuficiência de suas normas. Em razão disso, a fim de disciplinar os problemas decorrentes dos tratamentos de dados, se fez necessária a criação de uma nova lei intitulada de Lei Geral de Proteção de Dados. (GODINHO; NETO; TOLÊDO, p.05, 2020)

4.3 AMPLIAÇÃO DE PENAS PARA CRIMES CIBERNÉTICOS (LEI Nº 14.155/2021)

O presidente Jair Bolsonaro sancionou a lei 14.155/21, que amplia penas por crimes de furto e estelionato praticados com o uso de dispositivos eletrônicos como celulares, computadores e tablets.

O projeto altera o Código Penal e cria um agravante, com pena de reclusão de quatro a oito anos, para o crime de furto realizado com o uso desses aparelhos, estejam ou não conectados à internet, seja com violação de senhas, mecanismos de segurança ou com o uso de programas invasores.

A lei estabelece que, no crime de invasão de dispositivo informático previsto no Código Penal, tal penalidade passará a ser de reclusão, de um a quatro anos, e multa, aumentando-se a pena de um terço a dois terços se a invasão resultar em

prejuízo econômico. Nessa circunstância, a pena aplicável era de detenção de três meses a um ano e multa.

A medida determina também que, se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido, a pena passará a ser de reclusão, de dois a cinco anos, e multa. Até então, a pena em vigor neste caso era de reclusão, de seis meses a dois anos, e multa.

Se o crime for praticado contra idoso ou vulnerável, a pena aumenta de um terço ao dobro, considerando-se o resultado. E, se for praticado com o uso de servidor de informática mantido fora do país, o aumento da pena pode ir de um terço a dois terços.

No crime já existente de invadir aparelhos de informática para obter dados, modificá-los ou destrui-los, o projeto aumenta a pena de detenção de 3 meses a 1 ano para reclusão de 1 a 4 anos. A redação do tipo penal é alterada para definir que há crime mesmo se o usuário não for o titular do aparelho, condição comum no home office.

5. CONSIDERAÇÕES FINAIS

A presente monografia tem como principal objetivo explorar os crimes virtuais sob a ótica da legislação Brasileira, entretanto constatamos facilmente a dificuldade de delinear o espaço virtual e suas fronteiras. Verifica-se também por parte dos investigadores, legisladores e autoridades legais a falta de capacitação e conhecimento específico, para assim conseguir identificar, criar leis mais objetivas e punir os criminosos virtuais. (SILVA, 2012)

A sociedade de forma geral necessita de informações legais sobre os procedimentos de utilização da internet e de seus limites. O direito deve se apresentar de forma equivalente a velocidade de evolução da rede mundial de computadores. A atualização constante da ordem jurídica, somada aos mecanismos de prevenção e de repressão nos mostram que a criação de um direito específico não se faz necessário, mas sim, uma tipificação mais objetiva para tratar tais delitos. (MARTINS, 2017)

Por fim, e não menos considerável, é relevante denunciar os crimes virtuais, visto que hoje já é possível fazer uma denúncia através da própria internet. O Ministério Público Federal, através de seu site, oferece a ferramenta “Digidenuncia” que ao acessá-la o usuário pode optar em se identificar ou não. (NUCCIBER)

Em algumas cidades também as denúncias podem ser realizadas pessoalmente em delegacias especializadas em Crimes Cibernéticos, estes locais podem ser pesquisados no site do Instituto de Defesa Cibernética. Outra Forma de efetuar uma denúncia é através da “SaferNet” que é um órgão internacional que trabalha contra os crimes virtuais. A importância de se denunciar esse tipo de crime é muito necessária visto que muitos delitos acabam se repetindo por falta dela. (MARTINS, 2017)

REFERÊNCIAS

ARAS, Vladmir. **Informática Jurídica. Com. Crimes de informática. Uma nova criminalidade.** Disponível em: < http://www.informatica-juridica.com/trabajos/artigo_crimesinformticos.asp >

BARRETO, Alesandro Gonçalves, BRASIL, Beatriz Silveira. **Manual de Investigação Cibernética à luz do Marco Civil da Internet**. 1 Ed., São Paulo: Brasport, 2016.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. BRASIL, 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>.

BRASIL. **Lei nº 13.441, de 8 de maio de 2017.** Disponível em:<http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/L13441.htm>

BRASIL. Constituição (1988). Artigo 5, inciso XXXIX. PRESIDÊNCIA DA REPÚBLICA. CASA CIVIL. **Site do Planalto**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

BRITO, A. Direito Penal Informático. São Paulo: Saraiva, 2013

CAPEZ, Fernando. **Curso de Direito Penal – Parte Geral**. São Paulo, Editora Saraiva, 12 Ed. 2008.

CASTELLS, Manuel. **A galáxia da Internet**. Rio de Janeiro: Zahar, 2003. 178 p. Disponível em: <https://books.google.com.br/books?hl=pt BR&lr=lang_pt&id=nCKFFmWOnNYC&o>.

CÓDIGO PENAL BRASILEIRO. 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848. Acesso em 12 de maio de 2021.

CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA BRASILEIRA. 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em 10 de maio de 2021.

COSTA, Barbára. **O novo regulamento geral de proteção de dados (GDPR) da EU e o impacto dos negócios de ecommerce**. Disponível em: 27 de Janeiro de 2020. Acesso em: 05 de maio de 2021.

COSTA, D. O. R**. Lei antibaixaria: uma ponderação aos excessos da liberdade de expressão**. Revista Científica do Curso de Direito, [S. l.], n. 01, p. 131 - 146, 2017. DOI: 10.22481/rccd.v0i01.2706. Disponível em: . Acesso em: 05 de maio 2021.

D'URSO, Luiz Augusto Filizzola. **Cibercrime: perigo na internet.** Publicado em 2017. Disponível em . Acesso em 25 de maio de 2021.

FERREIRA, Ivette Senise. **A Criminalidade Informática. Direito & Internet – Aspetos Jurídicos Relevantes.** Editora Edipro, 2011, p. 261.

GODINHO, Adriano Marteleto; NETO, Genésio Rodrigues de Queiroga; TÔLEDO, Rita de Cássia de Morais. **A Responsabilidade Civil pela violação a dados pessoais.** Revista IBERC, v.3, n. 1, p. 1-23, jan.-abr./2020. Disponível em: . Acesso em: 18 de maio de 2021

GOMES, Luiz Flávio, Bianchini, Alice. **Crimes Informáticos e suas Vítimas**. 2 Ed., São Paulo: Saraiva, 2015.

https://ambitojuridico.com.br/cadernos/direito-penal/crimes-ciberneticos-consideracoes-sobre-a-criminalidade-na-internet/. Acesso em 20 de maio de 2021.

LEI DO MARCO CIVIL NA INTERNET, **LEI Nº 12.965/2014** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 19 de maio de 2021.

LEI DOS CIBERCRIMES, **LEI N° 12.737/12**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 10 de maio de 2021.

MORO, Tailane Moreno Delgado. **O que fazer frente a um vazamento de dados.** Disponível em: 1 de novembro de 2018. Acesso em: 20 de maio de 2021.

PANNAIN, Camila Nunes; PEZZELLA, Maria Cristina. Liberdade de Expressão e Hate Speech na Sociedade da Informação. **Revista Direitos Emergentes da Sociedade Global**, Santa Maria, v. 4, n.1, p. 72-87, 2015.

PINHEIRO, Patrícia Peck. Regulamentação da Web. **Cadernos Adenauer XV**, Rio de Janeiro, n. 4, p. 33-44, out/2014. Disponível em: < http://www.kas.de/wf/doc/16471-1442-5-30.pdf>

PINHEIRO, Patrícia Peck. **Direito Digital**. 4. Ed. São Paulo: Saraiva, 2010.p.65

PIOLI, Roberta Raphaelli. **Delitos Informáticos**: Lei Carolina Dieckmann traz inovações necessárias Revista Consultor Jurídico, abril 2013.

QUEIROZ, Tayrine. **Marco Civil da Internet: um estudo da sua criação sob a influência dos direitos humanos e fundamentais, a neutralidade da rede e o interesse público versus privado**. Disponível em: . 2015. Acesso em: 22 de maio de 2021.

QUINTINO, Eudes. **A nova lei Carolina Dieckmann.** Disponível em: https://eudesquintino.jusbrasil.com.br/artigos/121823244/a-nova-lei-carolina-dieckmann? 2012. Acesso em: 26 de abril de 2021.

ROSA, Fabrizio. **Crimes da Informática**. 2ª Ed. Campinas. Bookseller 2006.

ROZA, Anderson Figueira Da. **As redes sociais no mundo do crime.** 2016. Disponível em: canalcienciascriminais.com.br/as-redes-sociais-no-mundo-do-crime>

SANTOS, Gustavo de Oliveira; ANDRADE, Izabella Lucena Medeiros de; MORAIS, Lucas Andrade de. **A Responsabilidade Civil dos Estabelecimentos Fornecedores de Serviço de Acesso à Internet nos "Cybercrimes**". **Unieducar**, Fortaleza, ano XI, n. 4880, 2009.

SIQUEIRA, Marcela Scheuer et al. **Crimes virtuais e a legislação brasileira. (Re)Pensando o Direito** – Rev. do Curso de Graduação em Direito da Faculdade CNEC Santo Ângelo. v. 7, n. 13 (2017).

SOARES, Marcelo. **Maluf sofre sabotagem digital em e-mail**. Publicado em 2000. Disponível em . Acesso em 02 de maio de 2021.

SOARES, Will. **Denunciados por ofensas a Maju tinham verdadeiro exército, diz MP**. Publicado em 2016. Disponível em: http://g1.globo.com/saopaulo/noticia/2016/06/denunciados-por-ofensas-maju-tinham-verdadeiroexercito-diz-mp.html. Acesso em: 02 de maio de 2021.

TEIXEIRA, Tarcísio, **Direito Eletrônico**. 4º Ed. São Paulo: Joarez de Oliveira, 2007.

TOLEDO, Marcelo. **Hackers invadem sistema do Hospital do Câncer de Barretos e pedem regaste**. Publicado em 2017. Disponível em . Acesso em: 08 de maio de 2021.

TOMASEVICIUS FILHO, Eduardo. **Marco Civil da Internet: uma lei sem conteúdo normativo**. Estud. av., São Paulo, v. 30, n. 86, p. 269- 285, Abr. 2016. Disponível em. http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-40142016000100269&lng=en&nrm=iso

UPIS. **Crimes Cibernéticos: Como denunciar e qual a legislação no Brasil.** Disponível em: .23 de abril de 2019. Acesso em: 15 de maio de 2021.

VADE MECUM. 2020. 29º Ed. Editora Saraiva. Vários autores.

VIANNA, Túlio; MACHADO, **Felipe*. Crimes Informáticos.*** Belo Horizonte: Fórum, 2013.

WANDERLEY, Lucas Felix. **DELITO INFORMÁTICO E A LEI 12.737/12 (LEI CAROLINA DIECKAMNN).** Prof. Me. Ricardo Guilherme Corrêa da Silva, p. 34, 2014. Acesso em: 21 de maio de 2021.