CENTRO UNIVERSITÁRIO DE LAVRAS

A APURAÇÃO DOS CRIMES CIBERNÉTICOS E O DIREITO À INTIMIDADE

JÚLIA FURTADO CARDOSO

LAVRAS-MG

2019

JÚLIA FURTADO CARDOSO

A APURAÇÃO DOS CRIMES CIBERNÉTICOS E O DIREITO À INTIMIDADE

Monografia apresentada ao Centro Universitário de Lavras, como parte das exigências do curso de graduação em Direito.
Orientador: Prof. Me. Pedro Paulo Uchoa Fonseca Marques

LAVRAS-MG

2019

Ficha Catalográfica preparada pelo Setor de Processamento Técnico
da Biblioteca Central do UNILAVRAS

Cardoso, Júlia Furtado.
C268a A apuração dos crimes cibernéticos e o direito à intimidade / Júlia Furtado Cardoso; orientação de Pedro Paulo Uchoa Fonseca Marques. -- Lavras: Unilavras, 2019.
39 f.

Monografia apresentada ao Unilavras como parte das exigências do curso de graduação em Direito.

1. Crimes cibernéticos. 2. Direito à intimidade. I. Marques, Pedro Paulo Uchoa Fonseca (Orient.). II. Título.

Centro Universitário de Lavras – UNILAVRAS

Monografia intitulada **“A Apuração dos Crimes Cibernéticos e o Direito à Intimidade”**, de autoria da graduanda **Júlia Furtado Cardoso**, aprovada pela banca examinadora constituída pelos seguintes professores:

_____

Prof. Me. Pedro Paulo Uchoa Fonseca Marques – Unilavras (orientador).

_____

Prof. Me. Guilherme Scodeler de Souza Barreiro – Unilavras (presidente da banca).

Aprovada em _____ de _____ de _____

DEDICO,

Aos meus pais José Eustáquio e Lucíola.

Ao meu irmão Junior.

E a todos que, de alguma forma contribuíram para que eu chegasse a este momento.

RESUMO

Através do método analítico, mediante revisão de literatura, este estudo buscará, utilizando-se de fontes imediatas e mediatas do direito, quais sejam, as leis, doutrinas e princípios, e especialmente sob a ótica constitucional, analisar a apuração dos crimes cibernéticos, trazendo a conceituação do direito a intimidade, a honra, a imagem, a vida privada como direitos da personalidade, a era digital, a conceituação dos crimes cibernéticos, e as espécies. Traz também a homologação de leis buscando resguardar esses direitos, porém essas normas apresentam brechas, dentre as opiniões dos doutrinadores apresentados. Há necessidade da criação de uma agravante nos crimes informáticos, ocupando-se de um instrumento favorável para o cometimento de condutas ilícitas.

Palavras-chave: vida privada e intimidade; direito fundamental; crimes cibernéticos; ordenamento jurídico brasileiro.

LISTA DE SIGLAS E ABREVIATURAS

ART.	Artigo
CF	Constituição Federal
N.	Número
P.	Página
LGPD	Lei Geral de Proteção de Dados
GDPR	Regulamento Geral sobre a Proteção de Dados

SUMÁRIO

1 INTRODUÇÃO

Diante das grandes evoluções da era digital, o acesso a meios digitais se tornou de fácil ingresso aos cidadãos, trazendo benefícios, bem como consequências. A internet deixou de ser um lugar seguro, violando os direitos fundamentais através de invasões de dispositivos informáticos, divulgação de informações relacionadas a privacidade do usuário, bem como a divulgação de vídeos e fotos íntimas por meio da internet.

Contudo, cada dia que passa os usuários presenciam o abuso da sua privacidade na internet com certa constância. Isso se dá pelo motivo do anonimato que a internet conduza e se motiva a adotar o direito à liberdade expressão.

Por certo, com o avanço da internet no Brasil, as autoridades intuíram regulamentar o uso da internet e estabelecer direitos e deveres necessários para os usuários como para os provedores.

A Constituição Federal traz consigo os direitos e garantias fundamentais das pessoas o direito a inviolabilidade da sua privacidade e a proteção à sua liberdade de expressão.

A Lei 12.965/2014, surgiu para assegurar convívio da sociedade digital. A Lei Marco Civil da Internet como é conhecida essa lei, tem como objetivo resguardar a vida privada do cidadão e, ao mesmo tempo, preservar o direito à liberdade de expressão.

A privacidade assevera ao ser humano não ter o direito a intimidade e a vida privada expostas por terceiros sem a sua anuência.

Porém, o direito à liberdade de expressão é reconhecido também como direito à privacidade, sendo reconhecida pela lei 12.965/2014. Posto isto, caso extrapole a privacidade de terceiros, a vítima terá o direito de pleitear, demandando que o conteúdo seja retirado da internet.

Para tanto, o presente estudo encontra-se divido em tópicos. No primeiro, trata-se de uma breve consideração aos direitos a intimidade, a vida privada, a honra, e a imagem, na Constituição Federal.

À frente, foi necessário a conceituação e limitações dos direitos assegurados pelo artigo 5º, X da Constituição da República Federativa do Brasil, os quais são necessários para a distinção dessas figuras do texto Constitucional.

Ademais, indispensável a apresentação da conceituação dos crimes cibernéticos, sendo sua classificação como puros, mistos e os comuns, sendo necessário essa diferenciação, facilitando-se a compreensão dos crimes.

Então como continuação do tópico mencionado acima, são necessárias as especificações em relações as espécies dos crimes cibernéticos, visto que constituem ponto chave da pesquisa.

Por fim, mas de extrema importância, serão estudadas as três leis do ordenamento brasileiro referentes aos crimes cibernéticos, apresentados seus princípios, os direitos a serem protegidos, a punições e até mesmo brechas apresentadas em seus textos.

2 REVISÃO DE LITERATURA

2.1 Considerações Iniciais dos Direitos Fundamentais à Intimidade, a Vida Privada, a Honra e a Imagem, assegurados pela Constituição de 1988.

Com o advento da tecnologia, hoje a internet é considerada uma necessidade da era moderna, considerando –se que nos dias atuais não se vive mais sem, permitindo o acesso a uma quantidade de informações, pesquisas, estudos, abundantes, tornando-se as pessoas escravas da tecnologia. Por outro lado, traz consigo enormes problemas, como os ataques a vida privada e consequentemente a violação de direito fundamental previsto na Constituição da República Federativa do Brasil/88 (GREGO, 2016).

A Constituição Federal de 1988, deixa claro em seu artigo 5º, que todos os seres humanos são titulares de direitos fundamentais, sem distinção de qualquer natureza.

A Constituição da República Federativa do Brasil de 1988, no inciso X do art. 5º, assegura tanto as pessoas físicas e jurídicas, a inviolabilidade a intimidade, a vida privada, a honra e a imagem, compreendendo, como direito fundamental, pretendendo promover a dignidade da pessoa humana (MORAES, 2010).

“Os direitos à intimidade e à própria imagem formam a proteção constitucional à vida privada, salvaguardando um espaço íntimo intransponível por intromissões ilícitas externas” (MORAES, 2010, p. 53).

2.2 A Honra, a Intimidade, a Vida Privada e a Imagem como Direitos da Personalidade.

Aduz Faria (2009, p.118) que:

> Além de constituírem direitos fundamentais (com sua especial proteção pelo ordenamento jurídico) são ao mesmo tempo direitos da personalidade, isto é, essenciais à pessoa, inerentes a mesma e em princípio extrapatrimoniais. Na verdade, os direitos a honra, a intimidade, a vida privada e a imagem foram paulatinamente sendo perfilados primeiramente como direitos subjetivos da personalidade, com eficácia prevalente no âmbito inter privado para só mais tarde alcançar a estatura constitucional. Nessa ordem de ideias, cumpre mencionar a observação judiciosa realizada por *Durig*, de que os

> direitos da personalidade constituem mais audaz e o melhor impulso do direito privado nos últimos tempos.

Os direitos a personalidade são considerados indispensável e essencial, sendo um direito personalíssimo, estando na própria pessoa, como ser humano, sendo de direito desde o seu nascimento (FARIA, 2009).

2.2.1 Direito a Intimidade.

O conceito de intimidade, segundo Mendes, (2013, p.42):

> A intimidade é um sentimento que brota do mais profundo do ser humano, um sentimento essencialmente espiritual. É quase sempre considerado como sinônimo de privacidade, ou seja, uma terminologia de direito anglo americano (*right of privacy*), sendo a expressão direito a intimidade mais utilizada pelos povos latinos.

Reza o artigo 5º da Constituição Federal de 1988, ao convalescer a intimidade como dignidade da pessoa humana, considerando assim um direito inviolável, destarte: “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).

Para Dotti, (1998, p.69), a intimidade é “a esfera secreta da vida do indivíduo na qual este tem o poder legal de evitar os demais”.

Para Tavares (2015, p.531) “Significa a intimidade tudo quanto diga a respeito única e exclusivamente à pessoa em si mesma, a seu modo de ser e de agir em contextos mais reservados ou de total exclusão de terceiros”.

Ademais, Greco; Braga (2011) prelecionam que, com o advento do Direito Constitucional, que assegura os direitos fundamentais, traz como o centro o princípio da dignidade humana, guardando assim a relação com a intimidade e a vida privada, sendo que se não houvesse não teria amparo a nenhum outro direito. É importante ressaltar que estão ligados ao direito a intimidade, a inviolabilidade da casa (artigo 5º, XI), sigilo dos dados, das correspondências e das comunicações (artigo 5, XII) e o habeas data (artigo, 5º, LXXII).

2.2.2 Limites do Direito a Intimidade.

Ainda que o direito a intimidade esteja assegurado pela Constituição Federal de 1988, não será considerando absoluto, traz consigo algumas limitações.

Sampaio (1998, p. 379), aduz que:

> O direito a intimidade, não é, na prática, absoluto, encontrado suas fronteiras em outros direitos ou bens constitucionais. Essa limitação deverá ter por fundamento uma disposição constitucional, enunciadora de outro direito ou bem protegido.

Sampaio (1998), esclarece que a aludida restrição se faz diretamente, pelo meio de uma lei que sobrevenha sobre a área de proteção do direito a intimidade, sendo necessário uma outorga constitucional expressa. Como exemplo, a reserva de lei restritiva da inviolabilidade as comunicações telefônicas, preditas no artigo 5º, XII, da Constituição Federal de 1988.

Essas limitações também podem ser sofridas de forma indireta, que se materializa com a consolidação de outro direito (SAMPAIO, 1998).

Portanto, para que haja essa limitação é necessário um amparo jurídico, sendo que a norma precisará ser clara e necessita em suas disposições, haver adaptações, necessidade e proporcionalidade da medida.

2.2.3 Limites ao Direito da Privacidade.

Nas claras lições de Mendes (1994), a vivência em sociedade evita que se dê uma importância a privacidade. Considera-se que os interesses públicos, com amparo constitucional está em um nível elevado aos interesses individuais. O interesse público em muitas ocasiões pode ser estimulado por exato episódio ou por uma pessoa que vive uma imagem vinculada perante uma sociedade.

Cada caso deve ser levado em conta sobre a divulgação de informações de determinado ser humano, podendo ser considerada admissível ou abusiva. Desse modo é importante analisar como foi vinculada certa informação, se foi uma notícia obtida sem o consentimento da pessoa, violando assim a sua privacidade ou se foi livremente exposto pelo seu titular de direito (MENDES, 1994).

2.2.4 Distinções entre Intimidade e Vida Privada.

A distinção entre a intimidade e a vida privada é de difícil conceituação. A vida privada está ligada ao modo de ser, viver, conviver de cada pessoa, em público ou perante ele (TAVARES, 2015).

Para Mendes (1998, p.46), existe uma teoria para essa distinção:

> A vida particular ou privada poderia ser subdividida em outras esferas gradativamente menores, a proporção que a intimidade fosse restringindo. Na esfera maior, a vida privada passa-se os acontecimentos que o indivíduo não quer que se tornem públicos. Fora dessa esfera situam-se as ocorrências e condutas de natureza pública, ao alcance da coletividade em geral, não cabendo, aí, os delitos de indiscrição. A esfera da intimidade, ou esfera confidencial, está contida na esfera privada, é um círculo fechado de que tomam parte somente pessoas muitos íntimas. Por último, mais no centro, encontra-se a esfera do segredo, que deve ser protegida de toda forma de indiscrição. Dessa esfera não participam sequer pessoas da intimidade do sujeito: a necessidade de proteção contra a indiscrição é bem mais intensa.

Nos dias atuais, o direito à vida privada tem sido atingido cada dia que passa com o avanço tecnológico, com a instalação de aparelhos registradores de imagens, de dados e até de sons, tanto pelo setor privado como pelo Poder Público. Esse controle acaba violando a vida privada das pessoas (TAVARES, 2015).

Tavares (2015) ainda complementa, a intimidade consiste em a categoria mais protegida, cujo acesso é de vedação total, na maioria das vezes para familiares. Logo a vida privada ficará constituinte por uma categoria protetiva menor, ainda existente. Muitos podem ter acesso, mas isso não significa a possibilidade de divulgação irrestrita, massiva, ou a desnecessidade de autorização.

Sobre o conceito de intimidade, segundo, Moraes (2010) afirma que, de tal modo, a intimidade associa às relações subjetivas e de abordagem íntima do ser humano, suas afinidades com seus familiares e os de amizade. Enquanto a vida privada abrange os demais relacionamentos humanos, até mesmo os objetivos, como as relações comerciais, de trabalho, estudo e entre outros.

2.2.5 Direito a Honra.

A honra pode ser definida como as qualidades de cada ser humano, gerando um certo respeito pela sociedade, é aquele que resguarda sua honra pessoal, para o bom convívio entre os demais (TAVARES, 2015).

Conforme Canotilho (2013), há duas faces quando se fala ao direito a honra, quais são: subjetiva que está ligada a valoração que o ser humano faz de si mesmo, já a objetiva diz a respeito à reputação, prestigio e o bom nome que a pessoa tem interesse de fazer perante a sociedade.

2.2.6 Direito a Imagem

Tavares traz a composição da imagem como direito fundamental:

> A imagem é a apresentação, por desenho, impressão ou obra, de figura, pessoa ou coisa. Define-se direito à imagem como a tutela da imagem física da pessoa, contra ato que a reproduza ou a represente em fotografias, filmagens, retratos, pinturas, gravuras, aquarelas ou até mesmo escultura (TAVARES, 2015, p. 546).

O direito a imagem está assegurado pela Constituição Federal de 1988, em seu artigo 5º, XXVIII, ainda que apresente autorização para veiculação de imagem, a pessoa está protegida contra sua reprodução, infinita, salvo consentimento expresso ou contrato com a intenção, expressa ou implícita (TAVARES, 2015).

O direito a imagem deve ser observado de maneira ampla, quando está envolvido autoridades públicas, políticos, artistas, que na maioria das vezes a exposição à mídia, até mesmo pelos acontecimentos que abrangem essas pessoas, é exposto a conhecimento de todos (MORAES, 2007).

Tavares (2015), deixa claro que violado os direitos fundamentais, como a honra, imagem e a vida privada, cabe a vítima independente de ser uma pessoa conhecida no meio no social ou não, a partir do momento em há essa exploração busquem a tutela jurisdicional do estado cabível.

2.3 A Era Digital.

Com o avanço tecnológico nos meios de comunicações o objetivo de inventar uma aldeia global, admitindo que juntas as pessoas pudessem ter acesso a um fato de modo simultâneo (PINHEIRO, 2009).

Explica Pinheiro (2009, p.63) que:

> Este é o princípio que orienta a criação de redes mundiais de telejornalismo, como a CNN, além de toda uma rede *Broadcast* Digital para transmissões ao vivo e em tempo real, de qualquer lugar do mundo. O mundo financeiro também persegue essa mesma facilidade de comunicação investindo grandes somas na modernização dos equipamentos para permitir a criação de uma comunidade financeira mais dinâmica. Os chamados programas de *home-brokers* já são uma realidade. Seguindo a necessidade de corte de gastos e controles maiores sobre as filiais, as empresas passam a investir em redes de comunicações rápida, economizando papel, pulsos telefônicos, viagens e tempo.

Destaca Pinheiro (2009), que com a expansão desses benefícios para os lares, começa o movimento na era digital, com as compras de computadores para cada casa. Com esse avanço a tecnologia acaba expandindo para dentro dos lares, ligando assim a uma rede de consumidores por informações, serviços e produtos. Sendo que há uma grande vantagem para as empresas, levando em conta os custos operacionais, logísticas, vendas e distribuição, com uma maior eficiência.

Hoje o mundo está ligado a uma única aldeia e, ao mesmo tempo, agindo como nunca antes na história da humanidade (PINHEIRO, 2009).

Nesse sentindo dispõe Pinheiro (2009, p.61):

> Os mercados financeiros, como grandes precursores dessa era de convergência, foram os primeiros a sentir na pele as dificuldades desse universo. Se, por um lado, é muito bom estar conectado, por outro o comportamento irracional de mercado afeta a todos, onde quer que estejam de maneira nunca antes experimentada. A aludida complexidade é agravada pelo fator tempo, pela velocidade crescente com que os efeitos dessa rede de relações são sentidos em toda parte. Desde o início da era Mercantilista, os efeitos de uma crise local podiam ser sentidos em todo o mundo. Por exemplo, uma crise entre ingleses e chineses causada pelo comércio do chá no século XIX acarretava consequências na economia de todo o mundo, mas os efeitos dessa crise demoravam meses para chegar em todas as partes do planeta. Hoje, com a velocidade de transmissão de informações, tais efeitos são imediatos tanto em Londres como em São Paulo, no Cairo como em Sidney (PINHEIRO, 2009, p.61).

Nesta definição também explica Pinheiro, a necessidade que o ser humano tem da interatividade a nível global:

> A questão fica mais clara se refletirmos sobre um dos aspectos centrais da sociedade convergente: a interatividade, ou seja, a possibilidade de participação humana em um nível de inter-relação global. Vários avanços técnicos permitem que mais e mais pessoas atuem num mundo interativo: o movimento do *software* livre, de internet grátis, MP3, entre outros. A interatividade exige que as empresas virtuais

> estejam preparadas para atender seus consumidores e qualquer tempo e em qualquer lugar. No mundo virtual e interativo, uma empresa sediada em *Litle Rock, Arkansas*, vive com a possibilidade- e o risco- de interagir rapidamente com um consumidor, digamos, Mendonza, Argentina, numa realidade impecável há pouquíssimo tempo. Uma pessoa no interior de Goiás pode comprar e vender ações de uma empresa sediada na China com capital aberto na Bolsa de *Nova York*, EUA (PINHEIRO, 2009, p. 63).

O avanço tecnológico nos dias atuais vem crescendo cada dia mais, proporcionando assim um desenvolvimento tecnológico, possibilitando transmissões de imagens, sons e dados via satélite, onde em vários lugares do mundo podem ter acesso a uma informação ao mesmo tempo, tornando assim uma escala mundial da internet (PAESANI, 2013).

A internet é um meio de comunicação como os demais, rádio, televisão, telefone, fax, com isso não há em que se falar em Direito de Internet, mas sim em Direito Digital como um tipo de desafio é estar preparado para o desconhecido, seja aplicando as antigas ou novas leis, mas com a competência de interpretar a realidade social e adaptar as soluções aos acontecimentos com a mesma evolução da sociedade (PAESANI, 2013).

2.3.1 Direito Digital

Com o advento da tecnologia, o direito digital, abrange todos os princípios fundamentais, que são aplicados em todas áreas do direito. É importante ressaltar, que com esse avanço tecnológico mesmo abrangendo todos os princípios resguardados pela Constituição Federal, cabe aos profissionais do Direito, garantir o direito à privacidade, a proteção do direito autoral, o direito a imagem, da propriedade intelectual, dos *royalties*, da segurança da informação, dos acordos e parcerias estratégicas, dos processos contra *hackers* e entre outros. Posto isto, o direito digital deve ser entendido a criar novos instrumentos capazes de atender sua demanda (PINHEIRO, 2009).

Todos os meios de comunicações que compõem a sociedade nos dias atuais, passaram a ter uma grande importância no meio jurídico, a partir do momento em que se tornaram instrumentos de comunicação de massa que deverá ser abordada pelo direito, podendo causar insegurança no ordenamento jurídico e na sociedade (PINHEIRO, 2009).

Pinheiro, (2009, p.73), aduz que:

> O que propomos aqui, portanto, não é a criação de uma infinidade de leis próprias- como vimos, tal legislação seria limitada no tempo (vigência) e no espaço (territorialidade), dois conceitos que ganham dimensão em uma sociedade convergente. A proposta é que o direito siga sua vocação de refletir as grandes mudanças comportamentais vividas pela sociedade. No direito digital prevalecem os princípios em relação às regras, pois o ritmo de evolução tecnológica será sempre mais veloz que a atividade legislativa. Por isso a disciplina jurídica tende a auto-regulamentação, pela qual o conjunto de regras é criado pelos próprios participantes diretos do assunto em questão com soluções práticas que atendem ao dinamismo que a relações de direito digital exige.

Quanto as normas que estão ligadas ao direito digital, essas deverão ser publicadas no formato de avisos, como fazem os provedores, para que possibilite o maior conhecimento do público, aumentando assim sua eficácia (PINHEIRO, 2009).

É importante ressaltar que o direito digital não está somente ligado à internet, mas sim todas as outras inovações tecnológicas que estejam por vim.

Pinheiro, nesse sentindo conclui:

> Em tal realidade, o maior compromisso dos operadores do direito é evitar qualquer tipo de arbitrariedade. Por isso, a discussão dos projetos de lei sobre temas que envolvem informática, internet, e *e-commerce,* crimes virtuais devem ser feitos com a sociedade civil, envolvendo empresas e organizações sociais, para não cometermos o erro de desmoralizar a lei, desacreditando o direito (PINHEIRO, 2009, p.66).

Então como bem destaca Pinheiro (2009), o direito digital não pode ser considerado como novo. Ao contrário, tem ele seus amparos na maioria dos princípios do direito vigente além de aproveitar a maior parte da legislação atual.

Para Pinheiro (2009, p.66) “é errado pensar que a tecnologia cria um grande buraco negro, no qual a sociedade fica a margem do direito, uma vez que a leis em vigor são aplicáveis a matéria, desde que com sua devida interpretação”.

2.4 Crimes cibernéticos: Conceituação.

Para Ferreira (2000), o aparecimento dos crimes informáticos teve como marco histórico na época em que apareceram na imprensa e na literatura científica os primeiros usos de computadores para a pratica de delitos, de

manipulação, sabotagem, espionagem e o uso abusivo de computadores e sistemas denunciando assim as matérias jornalísticas.

Na década de 80, ressalta Ferreira (2000), que com o avanço significativo de ações criminosas que envolviam as manipulações de caixas bancárias, pirataria de programas de computadores, abusos nas telecomunicações, e até mesmo a pornografia infantil, entre outros, surgindo assim a vulnerabilidade que os inventores da tecnologia não tinham prevenido.

Muito se vem discutindo com o avanço tecnológico, situações a respeito dos chamados delitos de informática, que também são conhecidos como, crimes cibernéticos, crimes digitais, crimes de computadores, crimes via internet, entre outros (GREGO, 2016).

Ademais, segundo Grego (2016, p. 514):

> Na verdade, sob essa denominação se abrigam não somente os crimes em que o objeto material da conduta praticada pelo agente é um componente informático, a exemplo dos computadores ou as próprias informações existentes em um dispositivo informático, como também, e o que é mais comum, todas as demais infrações penais em que a informática é utilizada como verdadeiro instrumento para sua pratica.

Para Neto, Guimarães (2003), a informática deixa não só de cometer novos delitos como praticam os demais crimes previstos no Código Penal, através dos crimes cibernéticos.

Portanto, Neto, Guimarães (2003, p.69), “os crimes cometidos com os computadores (*The computer as tools of a crime*) e os cometidos contra o computador, isto é, contra as informações e programas neles contidos (*The Computer as the object of a crime)”.*

Primeiramente uma questão adiantada sobre os crimes digitais, que todas as informações arquivadas ou em trânsito por computadores, sendo que esses dados podem ser acessados ilicitamente, usados para ameaçar ou até mesmo para fraudes contra seus usuários (CORRÊA, 2000).

Os delitos da informática podem ser considerados como crimes virtuais puros, mistos e comuns.

Os crimes virtuais puros podem ser considerados aqueles que são praticados de forma ilícita que traga com si o sistema de computadores, suas informações, como os meios técnicos e físicos. Já os crimes virtuais mistos, é essencial para a sua consumação o uso da internet, como por exemplo os crimes

em que envolvem as transferências bancarias de forma ilícita, onde o invasor retira pequenas quantias de várias contas e transfere para apenas uma, transformando assim em uma expressiva quantia. Quando se fala dos crimes virtuais comuns, estamos diante do uso da internet para praticar um dos crimes já qualificados pelo Código Penal Brasileiro (PINHEIRO, 2009).

Para Ferreira (2000, p.210), “os crimes de informática é toda ação típica, antijurídica e culpável, cometida contra ou pela utilização de processamento automático de dados ou de sua transmissão”.

2.5 Direito à Intimidade e a Exposição de Informações na Internet.

Os crimes cometidos via internet, tem se tornado ilimitado, causando assim vários danos às vítimas. As discussões sobre os limites da liberdade de imprensa, a divulgação de informações, que estão ligados a intimidade, a vida privada, a imagem e a honra (MENDES, 1994).

A Constituição da República Federativa do Brasil de 1988, com o seu avanço, assegurou em seu artigo 5º, X, a inviolabilidade dos direitos fundamentais a intimidade, a vida privada, a honra e a imagem das pessoas, deixando claro que a punição não ocorrerá somente na esfera penal, confrontando também a lei hierarquicamente superior. Cabendo assim, como assegura a parte final “assegurado o direito a indenização pelo dano material ou moral, decorrente de sua violação”.

Na lição de Mendes (1994, p. 298), esclarece que:

> Se a constituição assegura, não só a inviolabilidade do direito, mas também a efetiva proteção judiciária contra a lesão, ou ameaça de direito (CF, Art. 5º, XXXV), não poderia o judiciário intervir para obstar a configuração da ofensa definitiva, que acaba acarretando danos efetivamente irreparáveis? Quais significaria a garantia da proteção judiciária efetiva contra lesão ou ameaça a lesão a direito se a intervenção somente pudesse se dá após a configuração da lesão? Pouco, certamente tão pouco!

O texto Constitucional de 1988 garantiu a liberdade de expressão como um direito absoluto, não podendo assim sofrer limites pelo poder judiciário e nem pelo poder legislativo. O artigo 220 da Carta Magna de 1988, traz que “a manifestação do pensamento, a criação, a expressão e a informação, sob

qualquer forma, processo ou veículo, não sofrerão qualquer restrição, observando o disposto nesta constituição". Posto isto, na Carta Maior não se descarta a probabilidade de que se colocassem limitações a liberdade de expressão e de comunicação, fundando expressamente que a liberdade se daria em concordância com o disposto na Constituição Federal de 1988.

A liberdade de informação jornalística para Mendes (1994), é mais expressiva, com relação ao artigo 220, parágrafo 1º da Carta Magna, sendo que "nenhuma lei conterá dispositivo que possa constituir embaraço a plena liberdade de informação jornalístico em qualquer veículo de comunicação social, observado o disposto no art.5º, IV, V, X, XIII, XIV".

Para Mendes (1994, p.298), o que parece contrário, mas de fato é um contorno que o legislador achou para fixar limites ao direito de liberdade a respeito de informações jornalísticas e a liberdade de pensamento.

> Como se vê, a formulação aparentemente negativa, contém, em verdade, uma autorização para o legislador disciplinar o exercício da liberdade de imprensa tendo em vista sobre tudo a proibição do anonimato, a outorga do direito de resposta e a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas. Do contrário não haveria razão para que se mencionassem expressamente esses princípios como limites para a liberdade de imprensa.

É importante ressaltar que, a lei traz limites a liberdade de expressão, levando em conta assegurar os direitos fundamentais e individuais não menos importante, como o princípio da dignidade da pessoa humana (MENDES, 1994).

Em outro lado para Mendes (1994, p.300), há um conflito entre a liberdade de informação e dos direitos amparados pelo artigo 5º, X, que assegura a proteção a vida privada e a intimidade:

> Como se vê, há uma inevitável tensão na relação entre a liberdade de expressão e de comunicação, de um lado, e os direitos da personalidade constitucionalmente protegidos, de outro, que pode gerar uma situação conflituosa, a chamada colisão de diretos fundamentais.

A garantia que está prevista a inviolabilidade da intimidade e a vida privada está diretamente ligado ao princípio da dignidade da pessoa humana, sendo este um dos princípios basilares da Constituição Federal, sendo assegurado no art. 1º, III da Constituição da República Federativa do Brasil.

Na visão de Santos (2014 apud OLIVEIRA, 2015, p.9).

> Em que pese o criticismo quanto aos efeitos do positivismo na perspectiva democrática, ressaltasse uma manifesta realidade: o acolhimento do ser humano, como valor supremo dos ordenamentos jurídicos, é uma tendência. Daí a noção de que a Dignidade Humana, seria, segundo alguns autores, o princípio valorativo máximo do Estado Democrático de Direito.

A dignidade da pessoa humana não nasceu do texto constitucional, mas sim uma criação de erros e acertos da humanidade num argumento de ações pelos movimentos sociais caracterizados por momentos específicos da história (MENDES, 1994).

2.6 Lei dos Crimes Virtuais: Análise da Lei 12.737/12.

Greco (2016), explana que a Lei 12.737, alterou o artigo 154-A do Código Penal, criando o tipo penal “invasão de dispositivo informático”.

A Lei 12.737/12, acrescentou no Código Penal Brasileiro, duas normas que tipificam os delitos cibernéticos.

Os artigos que foram alterados, estão presentes na seção no capítulo referente aos crimes contra a inviolabilidade dos segredos profissionais, sendo que são considerados delitos e não crimes (PAESINI, 2013).

A criação dessa nova lei, foi criada para acolher os anseios e necessidades da sociedade, sendo necessária a tutela de novos direitos. O caso ao qual se deu o primeiro passo para criação da Lei 12.737/12 foi o caso Carolina Dieckmann, invadiram seu dispositivo informático, considerando-se ser uma pessoa pública, o caso ganhou repercussão maior, sendo fundamental a aprovação da referida lei.

Posteriormente inúmeros acontecimentos levaram a exposição de pessoas exibindo a intimidade, em manifesta violação da intimidade e da vida privada, o legislador infraconstitucional, emitiu uma lei que aborda os crimes cibernéticos e a invasão de dispositivo informático (GREGO, 2016).

A era digital é conhecida em benefício do rápido e ininterrupto desenvolvimento tecnológico. Com o advento da tecnologia do conhecimento na sociedade tornou-se conectada, deste modo, certamente, tudo está ligado uma com a outra. Porém, com esse avanço foi desenvolvido um novo crime, o *cybercrime*, ou seja, os crimes cibernéticos (GRECO, 2016).

2.6.1 Ineficácia na Proteção à Intimidade na Lei 12.737/12.

A publicação da lei, designada para regular os crimes digitais no Brasil, foi somente o primeiro passo, pois as brechas no texto e a base deficitária da polícia podem confundir-se, tendo em vista o lapso temporal para prescrição dos crimes (GRECO, 2016).

Segundo Greco (2016, p.516), a Lei 12.737/12, exige a apresentação de certos meios, os efeitos de caracterização do delito de invasão dos dispositivos informáticos, sendo eles:

> Núcleo de invadir; b) dispositivo informático alheio; c) conectado ou não à rede de computadores; d) mediante violação indevida de mecanismo de segurança; e) com o fim de obter, adulterar ou destruir dados de informações sem autorização expressa ou tácita do titular do dispositivo; f) ou instalar vulnerabilidades para obter vantagem ilícita.

Sendo que para Greco (2016), o sentido de a palavra invadir está ligado ao de violar, penetrar e acessar.

Para Lucero e Kohen (apud, GRECO, 2016, p.516), informática é considerado:

> A ciência aplicada que trata o estudo e aplicação do processamento automático da informação, mediante a utilização de elementos eletrônicos e sistemas de computação. O termo *informatique* é acrônimo das palavras francesas *information e automatique*, o qual foi a utilizada pelo engenheiro Frances *Philipe Dreyfus* no ano de 1962 para a sua empresa *Societé d' Informatique Appliquée.*
>
> Posteriormente, esse termo começou a ser utilizado pelas diferentes línguas quando se desejava complementar a questão do processamento automático da informação. Sendo assim que ao ingressar no mundo castelhano, se conceitualizou a palavra informática. Para que se possa considerar um sistema informático se deve verificar necessariamente a realização das seguintes tarefas básicas: entrada: aquisição de dados. Processo: tratamento dos dados. Saída: transmissão dos resultados.

Portanto, para que ocorra o delito previsto no artigo 154-A do Código Penal, o dispositivo informático é todo aparelho capaz de receber informações, ocorrendo assim a transmissão dos resultados, como exemplos computadores, celulares e tabletes (GREGO, 2016).

O artigo 154-A exige que o dispositivo informático seja alheio, não podendo pertencer ao usuário. Posto isto, se uma terceira salva informações em

um computador de outra pessoa e se a mesma acessa os dados ali inseridos, não se caracteriza com o delito em tela (GRECO, 2016).

Aduz Greco (2016), que para que ocorra a infração penal de invasão de um dispositivo informático é necessário um dispositivo informático alheio, como exemplo um computador que não está ligado a qualquer rede, mas pode ser acessado através da internet.

Explica Greco (2016, p. 517):

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

Entende-se então, que a violação indevida de mecanismo de segurança, impossibilitar que alguma pessoa seja punida pelo tipo penal previsto no artigo 154-A do Código Penal, ainda que indevidamente, entre em dispositivo informático alheio sem que, para tanto, viole mecanismo de segurança, pois inexistente (GRECO, 2016).

Nessa sequência Greco (2016), deixa claro que raramente pessoas colocam senhas de acesso, em seus dispositivos informáticos, deixando assim, que qualquer pessoa tenha acesso, para conhecer o seu conteúdo. Todavia, mesmo sem a existência de senha de acesso, não é dado o direito de terceiros invadir computador alheio, a não ser que ocorra permissão expressa ou tácita de seu proprietário. Porém para que se configure delito, tendo em vista a exigência contida no texto legal em tela, somente haverá infração penal, se houver, por parte do agente invasor uma violação indevida do mecanismo de segurança.

Assevera Cunha (2015, p.263) “a ausência de dispositivo de segurança, ou o se não acionamento, impede a configuração típica”, ou ainda Coelho (2015, p. 69) “se o dispositivo informático não tiver mecanismo de segurança, não haverá tipicidade penal, posto que o legislador por não proteger a intimidade das pessoas que optam ou até mesmo, eventualmente esquecem de colocar senhas de segurança nos seus dispositivos informáticos”.

Para Greco (2016, p. 518), aquele que tem conhecimento e habilidades suficientes para violar mecanismo de segurança, invadindo dispositivo informático alheio, é conhecido como *hacker*:

> Este indivíduo, em geral, domina a informática, é muito inteligente, adora invadir sites, mas, na maioria das vezes, não com a finalidade de cometer crimes, costumam se desafiar entre si, para ver quem consegue invadir tal sistema ou página na internet, isto apenas para mostrar como estamos vulneráveis no mundo virtual.

Por outro lado, também existe o *cracker*, é aquele que:

> Usa a internet para cometer crimes, fraudes bancárias e eletrônicas, furto de dados, golpes e grandes estragos. São verdadeiras quadrilhas de jovens que não se contentam apenas em invadir um sistema, usam sua inteligência e domínio da informática para causar prejuízos de milhares de reais, tanto contra pessoas físicas, como jurídicas, órgãos públicos etc (NOGUEIRA, 2008, p.69).

A conduta do agente, ou seja, a ação de adentrar em dispositivo informático alheio, conectado ou não a rede de computadores, através de violação imprópria de mecanismo de segurança, necessita ser levado em conta o efeito obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo (GRECO, 2016).

Desta forma, a simples invasão, por intermédio de violação indevida de mecanismo de segurança, que implica na prática da infração penal tipificada no caput do artigo 154-A do diploma legal, entretanto, aquele que possui uma finalidade especial, ou seja, aquilo que nomeamos de especial de agir, que consiste na obtenção, adulteração ou destruição de dados ou informações sem autorização expressa ou tácita do titular do dispositivo (GRECO, 2016).

Aduz o artigo 154-A que a conduta de invadir dispositivo informático alheio, conectado ou não a rede de computadores, mediante violação indevida de mecanismo de segurança, pode ainda, além da intenção de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ser conduzida no sentido de instalar vulnerabilidades para conseguir vantagem ilícita (GRECO,2016).

De acordo com o centro de estudos, respostas e tratamentos de incidentes de segurança no Brasil, citado por Greco (2016, p. 519):

> Uma vulnerabilidade é definida como uma condição que, quando explorada por um atacante, pode resultar em uma violação de segurança. Exemplos de vulnerabilidades são falhas no projeto, na implementação ou na configuração de programas, serviços ou

> equipamentos de rede. Um ataque de exploração de vulnerabilidade ocorre quando um atacante, utilizando-se de uma vulnerabilidade, tenta executar ações maliciosas, como invadir um sistema, acessar informações confidencias, disparar ataques contra outros computadores ou tornar um serviço inacessível.

É importante salientar ainda, que de acordo com os estudos, reposta e tratamento de incidentes de segurança no Brasil, pode o agente instalar vulnerabilidades através dos chamados códigos maliciosos:

> Código malicioso (*malwares*) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador. Algumas das diversas formas como os códigos maliciosos podem infectar ou comprometer um computador são:
>
> Pela exploração de vulnerabilidade existentes nos programas instalados;
>
> Pelo auto execução de mídias removíveis infectadas, como *pen-drive;*
>
> Pelo acesso a páginas web maliciosas, utilizando navegadores vulneráveis;
>
> Pela ação direta de atacantes que, após invadirem o computador, incluem arquivos contendo códigos maliciosos;
>
> Pela execução de arquivos previamente infectados, obtidos em anexos mensagens eletrônicas, via mídias removíveis, em páginas web ou diretamente de outros computadores (através de compartilhamento de recurso)
>
> Uma vez instalados, os códigos maliciosos passam a ter acesso aos dados armazenados no computador e podem executarem ações em nome dos usuários, de acordo com permissões de cada usuário. Os principais motivos que levam um atacante a desenvolver e a propagar códigos maliciosos são a obtenção de vantagens financeiras, a coleta de informações confidenciais, o desejo de autopromoção e o vandalismo. Além disso, os códigos maliciosos são, muitas vezes, usados como intermediários e possibilitam a prática de golpes, a realização de ataques e a disseminação de spam (GRECO, 2016, p.520).

Os tipos previstos nos códigos maliciosos são: a) *vírus*- é um programa malicioso utilizado para replicar ou atacar os dispositivos informáticos. Para a efetivação do vírus é necessário a execução de arquivos que hospedam a se tornar ativos e continua o processo de infecção; b) *worm*- replica as mensagens sem o consentimento do usuário, alastrando programas, arquivos maldosos, ou congestionando a rede. É diferente do *vírus*, o *worm* são cópias de si mesmo em outros programas ou em arquivos. Seu alastramento se dá através da exploração existente ou as falhas na configuração de *softwares* instalados em computadores, os famosos cavalos de troia que na era digital, é conhecido como

uma programa espião, capaz de roubar informações, arquivos, senhas, entre outros, de determinado computador, abrindo portas para *hackers*; *spywares*- é considerado um programa espião que fornece informações dos computadores de um determinado usuário para redes desconhecidas, podendo ser coletados até mesmo através dos teclados e através de informações quando o usuários está online e também através dos e-mails, o *screenlogger* que é capaz de capturar a tela da área de trabalho do usuário, inclusive armazenando a posição do *cursor*; *bot*- é um programa usado para a comunicação do invasor, permitindo que seja controlado remotamente (GREGO, 2016).

Os códigos maliciosos são numerosos por meio dos quais podem ser praticados delito de invasão do dispositivo informático, a cada dia surgem diferentes formas de ataques (GRECO, 2016).

2.7 O Marco Civil da Internet.

O Marco Civil da Internet, deu início no Brasil com a discussão por meio de audiências públicas realizadas com a participação de grandes plataformas como o *Twiter*, *Facebook* e entre outros, através do portal da democracia, mantido pela Câmara dos Deputados, cuja a intenção é fundar princípios, garantias, direitos e deveres para o uso da Internet no Brasil, tendo a Lei 12.965/14- Marco Civil da Internet, sancionada pela Presidente Dilma Rousseff em abril de 2014 (OLIVEIRA, 2015).

Para Oliveira (2015), o documento é considerado uma “Constituição da Internet”, já que institui regras e conceitos básicos da rede, onde futuros projetos e leis terão seus fundamentos sobre o mundo digital. O texto traz a liberdade de expressão, a proteção à privacidade, a proteção de dados pessoais, a preservação da estabilidade, segurança e o estabelecimento da neutralidade da rede como princípios basilares da internet.

A presente lei traz um avanço significativo para a regulamentação da internet no Brasil (OLIVEIRA, 2015).

Aduz a Lei sobre os princípios, garantias e deveres para o uso da internet no Brasil:

> Art.18. O provedor de conexão com a internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros;

> Art.19. Com o intuito de assegurar a liberdade de expressão e impedir censuras, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial especifica, não tomar providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.
>
> (...)
>
> Art.21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo (BRASIL, 2014).

No que diz a respeito à proteção aos direitos constitucionais da honra, imagem e o reconhecimento do indivíduo, assegurado pelo Marco Civil, a retirada do conteúdo junto ao provedor da página, unicamente será de forma direta e imediata, se envolver nudez, cena de sexo, infração de direitos autorais ou a exposição de menor de idade. Todavia, quando se envolve outros fatos, a remoção do conteúdo, se dará por meio de ordem judicial, conseguindo, somente, a retirada parcialmente (OLIVEIRA, 2015).

A Lei traz que o acesso à internet é útil ao cidadão, e algum comportamento adverso aos bons costumes, que tenda denegrir a imagem, honra e privacidade do usuário, será punida.

O artigo 7º da Lei 12.965/14, conduz que:

> Art.7º. O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> I- inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
>
> II- inviolabilidade e sigilo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
>
> III- inviolabilidade e sigilo de suas comunicações provadas armazenadas, salvo por ordem judicial;
>
> IV- não suspensão de conexão à internet, salvo por débito diretamente decorrente de sua utilização;
>
> V- manutenção da qualidade contratada da conexão à internet;
>
> VI- informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso e aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;

> VII- não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
>
> VIII- informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para as finalidades que:
>
> a) justifiquem sua coleta;
>
> b) não sejam vedadas pela legislação; e
>
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
>
> IX- consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
>
> X-exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;
>
> XI-publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;
>
> XII-acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei;
>
> XIII-aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas pela internet (BRASIL,2014).

Aduz Oliveira (2015), que ao descobrir quem foi o agente do dano, do ilícito, para coibir esse tipo de crime e punir infratores, reverteu-se difícil, pois a configuração como está disciplinada na Lei 12.965/14, os provedores de conexão e aplicação não podem saber quais são os dados que estão armazenados no outro. Prontamente, é grande a probabilidade de não conseguir agregar o fato, a conduta, a uma identidade real e válida. As provas apenas são oferecidas pela via judicial. Vejamos:

> Art.10º. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que se trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
>
> §1º- O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. (BRASIL,2014).

Tendo em conta o andamento processual mais rápido, há previsão na referida lei de que as demandas, geralmente, tramitem nos Juizados Especiais.

Considerando que as demandas consumeristas estarão na fila, privilegiando os casos de difamação. Posto isto, o Poder Judiciário, suportará o acúmulo de processos, provocando morosidade nos processos e consequentemente, danos sociais (OLIVEIRA, 2015). É o que reza o artigo da referida lei:

> Art.19. Com o intuito de assegurar a liberdade de expressão e impedir a censura o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.
>
> (...)
>
> §3º- As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos para os provedores de aplicações de internet, poderão ser apresentados perante os juizados especiais (BRASIL,2014).

A referida lei traz como norma que um conteúdo só pode ser removido da internet depois de uma ordem judicial, e que o provedor não pode ser responsabilizado pelo conteúdo ofensivo publicado através de seu serviço por terceiros. A Lei Marco Civil, tem como escopo evitar a censura na internet, posto que para se provar que conteúdo é ofensivo, o responsável pela publicação deve ter o direito ao contraditório perante a Justiça (OLIVEIRA, 2015).

Para Varella (2014), a referida lei, traz consigo algumas exceções. Tendo em vista, que um conteúdo possa ser retirado do ar sem uma determinação judicial desde que viole uma norma penal, como exemplo pedofilia, racismo ou violência. Foi levado em conta que um conteúdo publicado possa causar riscos aos usuários, e que fique no ar enquanto aguarda uma deliberação de um juiz. Com isso, pretende-se mostrar que a internet ganhe mais segurança jurídica na retirada do conteúdo.

Para Pinheiro (2015), a Lei 12.965/14, é um grande passo para a segurança jurídica, porém ao se tirar do texto o que já tinha previsão na Constituição da República Federativa do Brasil/1988, no Código de Defesa do Consumidor, no Código Civil, no Código de Processo Civil, no Código Penal, o avanço pode ser considerando de uma forma simples para dar um tratamento apropriado a esta realizada que independe de territórios e de um conjunto de leis.

2.8 A Proteção de Dados Pessoais- Lei 13.709/18.

A causa para a criação da regulamentação da proteção de dados pessoais, se deu a partir dos anos 1990, com a expansão dos negócios econômicos por meio digital, passando a ter uma dependência maior dos fluxos internacionais de bases de dados, principalmente ligado às pessoas pelo avanço tecnológico (PINHEIRO, 2018).

Posto isto, foi necessário retomar o compromisso das instituições com os indivíduos, desta nova sociedade digital, no que diz a respeito à proteção dos direitos humanos, como a privacidade assegurada na Declaração Universal dos Direitos Humanos (DUDH) de 1948 (PINHEIRO, 2018).

Pinheiro (2018), destaca que a proteção das pessoas físicas em relação ao tratamento dos dados pessoais é um direito fundamental, previsto por diversas legislações em muitos países. No Brasil, se dá através da Lei do Marco Civil da Internet-12.965/14, porém a demanda garantida por essa lei, muitas vezes, notada de forma difusa e sem objetividade no tocante aos critérios que serão analisados adequados para motivar se houve ou não guarda, manuseio e descarte dentro dos padrões mínimos de segurança.

A nova legislação deu uma inovada neste aspecto, padronizando ou melhorando a normatização, trazendo características qualitativas a proteção de dados pessoais sem a presença dos quais haveria penalidade (PINHEIRO, 2018).

Aduz Pinheiro (2018), que a LGPD em algumas partes deixou uma interpretação mais ampla, carregando consigo uma insegurança jurídica, permitindo um espaço para o pessoal onde deveria ter sido mais assertório. Como exemplo a determinação de prazo, a LGPD prevê um prazo razoável.

Ademais, para Pinheiro (2018, p.22) “além disso, houve o veto presidencial no tocante à criação da Autoridade Nacional de Proteção de Dados Pessoais e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade”.

O veto a criação da autoridade e do conselho responsável pela proteção dos dados pessoais, gera uma dificuldade para a regulamentação da norma, considerando um problema para a fiscalização, podendo ter legitimidade o

Ministério Público, capaz de gerar alguns entraves, considerando ser uma matéria nova e de ordem técnica elevada, e atrapalhando também a criação das relações comerciais no Brasil (PINHEIRO, 2018).

A lei traz um rol de princípios a ser atendidos que são considerados necessários. Portanto, a presente regulamentação tende a proteção da privacidade do titular dos dados, a liberdade de expressão, de informação, de opinião e de comunicação, a inviolabilidade da intimidade, da honra e da imagem e o desenvolvimento econômico e tecnológico (PINHEIRO, 2018).

Em relação as penalidades, ressalta Pinheiro (2018), sofreram alguns vetos presidenciais, acolhendo a necessidade de adaptação para a fato e o contexto do cenário econômico e social do Brasil.

Foram previstas as seguintes penalidades administrativas, devendo observar alguns requisitos, como exemplo o da proporcionalidade:

> Art. 52- Os agentes de tratamento de dados, em razão das infrações cometidas às normas prevista nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
>
> I- advertência, com indicação de prazo para adoção de medidas corretivas
>
> II- multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercícios, excluídos os tributos, limitada, no total, a R$50.000.000,00 (cinquenta milhões de reais) por infração
>
> III- multa diária, observando o limite total a que se refere o inciso II;
>
> IV- publicização da infração após devidamente apurada e confirmada a sua ocorrência;
>
> V- bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
>
> VI- eliminação dos dados pessoais a que se refere a infração;
>
> VII- suspensão parcial ou total do funcionamento do banco de dados, a que se refere a infração pelo período até a regularização da atividade de tratamento pelo controlador;
>
> VIII- suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6(seis) meses, prorrogável por igual período;
>
> IX- proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados (BRASIL, 2018).

Desta forma, o programa de gestão de dados pessoais bem executado ajudaria na redução das penas, na presunção de ocorrência de um tipo de infração que facilitaria a aplicação de alguma penalidade (PINHEIRO, 2018).

Para Pinheiro (2018, p.36), alguns itens podem ser considerados para minorar uma punição advertida pela Autoridade Fiscalizadora responsável:

> A gravidade da infração; A boa-fé do infrator; A vantagem auferida; A condição econômica do infrator; A reincidência; O grau de dano causado; A cooperação do infrator; A demonstração de adoção de mecanismo e procedimentos para mitigar os danos; A adoção de política de boas práticas e governança; A pronta adoção de medidas corretivas; A proporcionalidade entre a gravidade da falta e a intensidade da sanção.

Posto isto, é preciso focar nos princípios que asseguram a Lei Geral de Proteção de Dados para que a norma seja suportável (PINHEIRO, 2018).

2.8.1 Análise Comparativa com Regulamento Europeu.

Tendo em conta a comparação entre a LGPD e o GDPR, ambas as leis tem como objetivo o tratamento de dados pessoais, assegurando os direitos fundamentais das pessoas naturais (PINHEIRO, 2018).

Posto isto, é importante ressaltar que a Lei 13.709/18, é uma nova legislação brasileira trazendo grande impulso para as instituições privadas e públicas abordando os dados pessoais dos indivíduos em qualquer relação que abranja o tratamento de informação consideradas como dados pessoais (PINHEIRO, 2018).

A LGPD, é uma das leis mais técnicas presente no ordenamento jurídico, congregando uma série de itens de controle para afirmar as garantias previstas na proteção dos direitos humanos (PINHEIRO, 2018).

O prazo estabelecido para a vigência da presente lei é de 18 meses, atendendo o grande impacto econômico e social, recebendo a necessidade de atender todas as exigências de forma eficiente e sustentável, atingindo um nível de proteção de dados tanto no âmbito nacional como no Internacional, exigindo assim uma política pública para ser implementada (PINHEIRO, 2018).

A criação da presente lei, foi estabelecida para a proteção dos direitos fundamentais da liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural, trazendo alegação da boa-fé para todo o tipo de tratamento de dados pessoais, passando a cumprir uma série de princípios, e por outro lado, os controles técnicos para a proteção das informações (PINHEIRO, 2018).

3 CONSIDERAÇÕES GERAIS

O presente estudo tem como propósito de apurar se os crimes cibernéticos violam os direitos fundamentais previstos no artigo 5º da Constituição da República Federativa do Brasil, como o direito a intimidade, a vida privada, a honra e a imagem.

Desta forma, de início, foi necessário apresentar as considerações referentes aos direitos fundamentais a intimidade, a vida privada, a honra e a imagem, que são asseguradas pela Constituição Federal de 1988 em conflito com o avanço tecnológico, violando os direitos fundamentais.

Logo em seguida foi apresentado os direitos a honra, a intimidade, a vida privada e a imagem como direitos da personalidade, considerando que são direitos personalíssimos, sendo adquiridos pelo ser humano desde o seu nascimento.

Diante disso, foi exposto o conceito do direito a intimidade, que diz tudo a respeito à vida única e exclusivamente da pessoa, considerando o seu modo de agir em contextos mais particulares. Contundo, o direito a intimidade não é considerado absoluto, trazendo consigo limitações para a sua aplicação.

Assim, foi necessário realizar uma pesquisa em relação a distinção entre o direito a intimidade e a vida privada, sendo que a vida privada está ligada ao modo de ser e viver de cada pessoa, já a intimidade é a relação pessoal do ser humano, como a afinidade com seus familiares e amigos.

Neste sentido, necessária também se fez a análise e conceituação dos direito a honra tendo em vista, conforme verificou é considerado uma qualidade de cada pessoa, para um bom convívio na sociedade. Já o direito a imagem está ligado a toda imagem física da pessoa.

A frente adentrou-se a era digital que vem avançando cada dia mais, com os avanços tecnológicos, crescendo como nunca visto antes. O direito digital abrange todos os princípios fundamentais que são aplicados nas áreas de direitos, não havendo distinção entre os direitos a internet e os demais direitos ligados aos outros meios de comunicações.

Logo após, e sendo de suma importância veio a conceituação dos crimes cibernéticos, que são considerados crimes cometidos via internet ou pelo computador. Podem ser considerados crimes puros, aqueles atentados de forma ilícita contra as informações como os meios técnicos e físicos dos sistemas de computadores. Os crimes mistos para que ocorra a sua consumação é necessário uso da internet. Por fim, os crimes virtuais comuns, que são os crimes previsto no Código Penal Brasileiro, que são cometidos pelo uso da internet.

E por fim, foi apresentado os tipos de crimes cibernéticos, reconhecidos pela Organização das Nações Unidas, sendo possível perceber que os crimes informáticos de forma direta e indireta violam os direitos previstos na Constituição Federal de 1988, através de invasões de computadores, divulgação de fotos e vídeos íntimos sem o consentimento da vítima, sendo que os crimes virtuais têm se tornado ilimitado, causando vários danos aos usuários.

Desta maneira, foi analisada as leis que punem os criminosos que praticam os crimes cibernéticos, são elas: Lei 12.737/12, alterando alguns artigos do Código Penal, porém apresentando brechas no texto. A Lei marco civil da internet, a presente lei foi considerada como uma “constituição da internet” instituindo regras e conceitos básicos para a criação das futuras leis. E por fim, a Lei Geral de Proteção de Dados, que entrará em vigor em fevereiro de 2020, porém antes mesmo de entrar em vigor já apresenta algumas falhas, como o veto presidencial em relação a criação de um órgão técnicos especializado para a fiscalização de proteção de dados pessoais pelo Estado e algumas partes deixando a interpretação mais ampla.

Portanto, os crimes cibernéticos violam os direitos fundamentais a intimidade, a vida privada, a honra e a imagem, não tendo uma lei eficaz capaz de cumprir os ditames legais e resguardar os princípios fundamentais previstos na Carta Maior.

4 CONCLUSÃO

Através da pesquisa, foi possível concluir que os benefícios trazidos pela internet não podem ser negados, porém os usuários correm um certo risco envolvendo a violação ao direito a intimidade, a honra, a vida privada e a imagem. O Brasil passou a reconhecer o surgimento de novos bens jurídicos passando a tutelar primeiramente através da criação da Lei 12.737/12, alterando o artigo 154-A do código penal brasileiro. Logo após veio a necessidade da criação da Lei 12.965/14, assegurando os princípios, garantias, direitos e deveres do uso da internet, observando de forma mais difusa e sem objetividade e pôr fim a criação da Lei Geral de Proteção de Dados que ainda não está em vigor, dispondo sobre a proteção de dados pessoais, alterando a lei 12.965/14.

Assim, conclui-se que os crimes cometidos via internet ou pelo computador, violam os direitos fundamentais previstos na Constituição Federal de 1988, através de manipulações de dados pessoais, sejam através de imagens, sons, vídeos, invasões em dispositivos informáticos, programas instalados nos computadores com uma única finalidade de invasão para coleta de dados, senhas, e entre outros.

Então, após a pesquisa, afirma-se que, as legislações pertinentes, pecou, deixando de proteger os direitos fundamentais a intimidade, a vida privada, a honra e a imagem, asseguradas pela Constituição da República Federativa do Brasil, considerando que a proteção desses direitos sobre o aspecto privado das pessoas, e os limites desses direitos, visto que nenhum direito é considerado absoluto, sendo que a divulgação de imagens ou informações de determinadas pessoas podem ser abusivas ou aceitáveis.

Contudo, foram identificados mais pontos negativos do que positivos, considerando que a Lei 12.373/12, traz uma interpretação em relação ao termo “invadir “ambíguo. Já o termo “mecanismo de segurança” remete a ideia de proteção quanto a invasão, que se concretiza a partir da instalação de hardware como antivírus, spywares, firewall, senhas de segurança, faz com que o dispositivo esteja desprotegido e consequentemente não há que se falar em

crime, uma vez que não houve a violação do mecanismo de segurança. E por fim traz que se o agente não tem intenção de obter dados, mas somente por curiosidade, invade dispositivo informático, ou tenta-lo faze-lo, essa conduta não se enquadra no artigo 154-A do Código Penal.

Já a Lei que trata do Marco Civil da internet é considerada pelos doutrinadores observada de forma difusa e sem objetividade no tocante aos critérios que serão estimados correspondentes para definir se houve ou não guarda, manuseio e descarte dos padrões mínimos de segurança condizentes.

A Lei Geral de Proteção de Dados antes mesmo de entrar em vigor, em alguns aspectos deixou a margem de interpretação mais ampla, apresentando alguns pontos de insegurança jurídica por permitir um espaço mais subjetivo onde deveria ter sido mais assertiva. Além disso, houve o veto presidencial para a criação da Autoridade Nacional de Proteção de Dados Pessoais e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, deixando de criar um órgão técnico responsável pela fiscalização, podendo dificultar aplicação da lei e uma limitação nas relações comerciais no Brasil.

Desta maneira, conclui-se que os crimes cibernéticos, não é completamente imprescindível, mas cabe aos futuros estudantes de direito a continuação das pesquisas acadêmicas, para atingir um maior grau de eficácia na aplicação das leis, preservando os princípios e fundamentos do estado democrático de Direito.

REFERÊNCIAS BIBLIOGRÁFICAS

BRASIL. **Código Penal Brasileiro**. Brasília: Senado Federal, 2002. Vade Mecum Saraiva. 24ª.ed. São Paulo: Saraiva, 2017.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília: Senado Federal, 1988. Vade Mecum Saraiva. 24ª.ed. São Paulo: Saraiva, 2017.

BRASIL. **Lei 12.965**. Brasília: Senado Federal, 2014. Vade Mecum Saraiva. 24ª.ed. São Paulo: Saraiva, 2017.

CANOTILHO, J.J. Gomes. Et al. **Comentários a Constituição do Brasil.** – São Paulo: Saraiva, 2013.

CUNHA, Rogério Sanches, **Direito Penal- Parte Geral**. Atlas. São Paulo. 2013.

COELHO, Yuri Carneiro. Curso de Direito Penal Didático. Atlas. 2ª Ed. São Paulo, 2015.

CORREA, Gustavo Testa. **Aspectos Jurídicos da Internet.** Saraiva. São Paulo, 2000.

CUNHA, Sanches Rogério. Manual do Direito Penal. JusPodim. 3ª Ed. Salvador, 2015.

DOTTI, René Ariel. **Proteção da Vida Privada e Liberdade de Informação.** Editora RT. São Paulo, 1998.

FARIA, Edilson Pereira. **Colisão de Direitos**. Sergio Antônio Fabris Editor. 3ª. Ed. São Paulo, 2009.

FERREIRA, Ivete Senise. **A Criminalidade Informática**. Edipro. São Paulo. 2000.

GRECO, R; BRAGA, R.R.P**. Da Principiologia Penal ao Direito a Intimidade como Garantia Constitucional. Revista Direito e Desenvolvimento. A. 2. N. 4, 2011.**

GRECO, Rogério. **Curso de Direito Penal**. Impetus. Ed 13ª. São Paulo, 2016.
MENDES, Gilmar Ferreira. **Curso de Direito Constitucional**. Atual.8ª Ed. São Paulo, 2013.

MENDES, Gilmar Ferreira. **Direitos e garantias individuais/ Direito da Personalidade/Liberdade de Expressão**. **Revista de informação legislativa. v.13, nº122, p.297-301, abr./jun, 1994.**

MENDES, Maria Gilmaíse Oliveira de. Direito a Intimidade e a Vida Privada. Del Rey, São Paulo, 1998.

MORAES, Alexandre de. **Constituição do Brasil Interpretada e Legislação Constitucional**. 7. Ed. Atualizada até a EC Nº55/07 – São Paulo: Atlas, 2007.
MORAES, Alexandre de. **Direito Constitucional**. Atlas. 26ª. Ed. São Paulo, 2010.

NETO, M.F; GUIMARÃES, J.A.C. **Crimes na Internet: Elementos para uma reflexão sobre a ética informacional**. **R.CEJ, Brasília, nº 20, p.67-73, jan./mar. 2003.**

NOGUEIRA, Sandro D´ Amato. **Crime Informático**. BH Editora. 2ª Ed. Belo Horizonte. 2008.

OLIVEIRA, Carlos Eduardo Elias de. **Aspectos Principais da Lei nº 12.965/2014, o Marco Civil da Internet: Subsídios a Comunidade Jurídica.** Senado Federal. Brasília, 2014.

PAESANI, Liliana Minardi. **Direito e Internet**. Atlas. São Paulo. 2013.

PAESANI, Liliana Mirardi. **Direito e Internet**. Atlas. São Paulo, 2013.

PINHEIRO, Patrícia Peck. **Direito Digital**. 4ª edição. Saraiva, 2009 Saraiva, São Paulo.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais Comentários à Lei nº 13.709/2018 (LGPD).** Saraiva. São Paulo, 2018.

SAMPAIO, José Adércio Leite. **Direito a Intimidade e a Vida Privada**. Del Rey. São Paulo, 1998.

OLIVEIRA, Claudio Roberto de Almeida. **A Intimidade da Sociedade Digital e a Eficácia da Lei 12.737/12 – Invasão de Dispositivo Informático.** Conteúdo jurídico, Brasília. 2015.

TAVARES, André Ramos. **Curso de Direito Constitucional**. Saraiva. 13ª. Ed. São Paulo, 2015.