UNIVERSIDADE FEDERAL DE GOIÁS
UNIDADE ACADÊMICA ESPECIAL DE CIÊNCIAS SOCIAIS APLICADAS
GRADUAÇÃO EM DIREITO

VICTOR HUGO ARAÚJO DE SOUSA

CRIMES ELETRÔNICOS TIPIFICADOS NA LEI BRASILEIRA FACE AO MARCO CIVIL DA INTERNET (LEI Nº 12.965/2014) E À LEI GERAL DE PROTEÇÃO DE DADOS (LEI Nº 13.709/2018)

Cidade de Goiás
2021

UNIVERSIDADE FEDERAL DE GOIÁS
UNIDADE ACADÊMICA ESPECIAL DE CIÊNCIAS SOCIAIS APLICADAS

TERMO DE CIÊNCIA E DE AUTORIZAÇÃO PARA DISPONIBILIZAR VERSÕES ELETRÔNICAS DE TRABALHO DE CONCLUSÃO DE CURSO DE GRADUAÇÃO NO REPOSITÓRIO INSTITUCIONAL DA UFG

Na qualidade de titular dos direitos de autor, autorizo a Universidade Federal de Goiás (UFG) a disponibilizar, gratuitamente, por meio do Repositório Institucional (RI/UFG), regulamentado pela Resolução CEPEC no 1240/2014, sem ressarcimento dos direitos autorais, de acordo com a Lei no 9.610/98, o documento conforme permissões assinaladas abaixo, para fins de leitura, impressão e/ou download, a título de divulgação da produção científica brasileira, a partir desta data.

O conteúdo dos Trabalhos de Conclusão dos Cursos de Graduação disponibilizado no RI/UFG é de responsabilidade exclusiva dos autores. Ao encaminhar(em) o produto final, o(s) autor(a)(es)(as) e o(a) orientador(a) firmam o compromisso de que o trabalho não contém nenhuma violação de quaisquer direitos autorais ou outro direito de terceiros.

1. Identificação do Trabalho de Conclusão de Curso de Graduação (TCCG)

Nome(s) completo(s) do(a)(s) autor(a)(es)(as): **VICTOR HUGO ARAÚJO DE SOUSA**

Título do trabalho: **CRIMES ELETRÔNICOS TIPIFICADOS NA LEI BRASILEIRA FACE AO MARCO CIVIL DA INTERNET (LEI Nº 12.965/2014) E À LEI GERAL DE PROTEÇÃO DE DADOS (LEI Nº 13.709/2018)**

2. Informações de acesso ao documento (este campo deve ser preenchido pelo orientador) Concorda com a liberação total do documento [X] SIM [ ] NÃO[1]

[1] Neste caso o documento será embargado por até um ano a partir da data de defesa. Após esse período, a possível disponibilização ocorrerá apenas mediante: a) consulta ao(à)(s) autor(a)(es)(as) e ao(à) orientador(a); b) novo Termo de Ciência e de Autorização (TECA) assinado e inserido no arquivo do TCCG. O documento não será disponibilizado durante o período de embargo.

Casos de embargo:

- Solicitação de registro de patente;

- Submissão de artigo em revista científica;

- Publicação como capítulo de livro.

Obs.: Este termo deve ser assinado no SEI pelo orientador e pelo autor.

Documento assinado eletronicamente por **Bruna Pinotti Garcia Oliveira**, **Professora do Magistério Superior**, em 13/11/2021, às 10:39, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **VICTOR HUGO ARAUJO DE SOUSA**, **Discente**, em 13/11/2021, às 10:44, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Referência: Processo nº 23070.055790/2021-75 SEI nº 2489331

VICTOR HUGO ARAÚJO DE SOUSA

CRIMES ELETRÔNICOS TIPIFICADOS NA LEI BRASILEIRA FACE AO MARCO CIVIL DA INTERNET (LEI Nº 12.965/2014) E À LEI GERAL DE PROTEÇÃO DE DADOS (LEI Nº 13.709/2018)

Monografia jurídica apresentada à Unidade Acadêmica Especial de Ciências Sociais Aplicadas da Regional Goiás da Universidade Federal de Goiás, como trabalho de conclusão do curso de bacharelado em Direito, sob a orientação da Profa. Dra. Bruna Pinotti Garcia Oliveira.

Cidade de Goiás
2021

Ficha de identificação da obra elaborada pelo autor, através do
Programa de Geração Automática do Sistema de Bibliotecas da UFG.

Sousa, Victor Hugo Araújo de
CRIMES ELETRÔNICOS TIPIFICADOS NA LEI BRASILEIRA FACE AO MARCO CIVIL DA INTERNET (LEI Nº 12.965/2014) E À LEI GERAL DE PROTEÇÃO DE DADOS (LEI Nº 13.709/2018) [manuscrito] / Victor Hugo Araújo de Sousa. - 2021.
58 f.

Orientador: Profa. Dra. Bruna Pinotti Garcia Oliveira.
Trabalho de Conclusão de Curso (Graduação) - Universidade Federal de Goiás, Unidade Acadêmica Especial de Ciências Sociais Aplicadas, Direito, Cidade de Goiás, 2021.

1. Cibercrimes. 2. Marco Civil da Internet. 3. Lei Geral de Proteção de Dados. 4. Avanço tecnológico. 5. Segurança da informação. I. Oliveira, Bruna Pinotti Garcia, orient. II. Título.

CDU 343

UNIVERSIDADE FEDERAL DE GOIÁS
UNIDADE ACADÊMICA ESPECIAL DE CIÊNCIAS SOCIAIS APLICADAS

ATA DE DEFESA DE TRABALHO DE CONCLUSÃO DE CURSO

Aos 29 dias do mês de outubro do ano de 2.021 iniciou-se a sessão pública de defesa do Trabalho de Conclusão de Curso (TCC) intitulado "CRIMES ELETRÔNICOS TIPIFICADOS NA LEI BRASILEIRA FACE AO MARCO CIVIL DA INTERNET (LEI Nº 12.965/2014) E À LEI GERAL DE PROTEÇÃO DE DADOS (LEI Nº 13.709/2018)", de autoria de VICTOR HUGO ARAÚJO DE SOUSA, do curso de Direito, da Unidade Acadêmica Especial de Ciências Sociais Aplicadas da UFG. Os trabalhos foram instalados pela presidente, Profa. Dra. Bruna Pinotti Garcia Oliveira – orientadora (UAECSA/UFG) com a participação dos demais membros da Banca Examinadora: Profa. Ma. Renata Botelho Dutra (UAECSA/UFG) e Profa. Ma. Flávia Ribeiro da Silva. Após a apresentação, a banca examinadora realizou a arguição do estudante. Posteriormente, de forma reservada, a Banca Examinadora deliberou e considerou o TCC aprovado.

Proclamados os resultados, os trabalhos foram encerrados e, para constar, lavrou-se a presente ata que segue assinada pelos Membros da Banca Examinadora.

Documento assinado eletronicamente por **Bruna Pinotti Garcia Oliveira**, **Professora do Magistério Superior**, em 13/11/2021, às 10:11, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **FLÁVIA RIBEIRO DA SILVA**, **Usuário Externo**, em 13/11/2021, às 10:27, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Renata Botelho Dutra**, **Professora do Magistério Superior**, em 13/11/2021, às 11:16, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.ufg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2489313** e o código CRC **1AB15BBC**.

Referência: Processo nº 23070.055790/2021-75 SEI nº 2489313

AGRADECIMENTOS

Agradeço primeiramente a Deus por ter guardado a mim e a minha família nesses tempos difíceis, e ter concedido a força necessária para caminhar até aqui.

Aos meus pais, Elton Messias e Francisca Araújo, que sempre estiveram ao meu lado, se esforçaram, se sacrificaram, trabalhando arduamente em prol da minha formação acadêmica, sem esse apoio nada disso seria possível.

À minha companheira Cáritha Caroline, minha grande incentivadora e parceira durante esses anos de formação, contribuindo sempre com a minha evolução e crescimento.

Também à sua família que tiveram um papel fundamental no meu bem estar durante o período de curso na Cidade de Goiás.

À minha irmã Anna Victoria, grande amiga e base importante na minha vida.

Aos meus familiares pelas orações e toda assistência prestada.

À minha orientadora, Bruna Pinotti que grandiosamente forneceu todo o amparo necessário para o desenvolvimento dessa pesquisa.

“Aprender é a única coisa de que a mente nunca se cansa, nunca tem medo e nunca se arrepende.”.
(Leonardo da Vince)

RESUMO

Cibercrimes, crimes informáticos ou crime virtual, os nomes dos crimes via Internet ao longo dos anos, tornaram-se populares com o avanço da conexão pela sociedade, o que se deve às várias formas de interação entre os indivíduos que surgiram ao longo dos anos. Da mesma forma que o surgimento de novas formas de interações entre os usuários, novas formas de crime surgiram em proporções semelhantes. O objetivo primário desse trabalho é deixar claro o crescimento de forma descontrolada dessa modalidade de crime, propiciado pela nossa economia moderna, veloz e dinâmica, enaltecida pelo avanço das tecnologias e os benefícios da era digital. Com o objetivo de divulgar e cumprir o papel da educação social, é destacado o crescimento dos incidentes de segurança no país, mostrando que as pessoas e as organizações aprenderam sobre os riscos que enfrentam. Por fim, fora analisado as ameaças do mundo digital, na qual pessoas e organizações precisam estabelecer conexões seguras e interagir diante relações comerciais e institucionais, aplicando boas práticas de segurança, com a apresentação de legislações específicas que se tornaram necessárias para a regulamentação e punição de cibercrimes.

Palavras-chave: Cibercrimes. Marco Civil da Internet. Lei Geral de Proteção de dados. Avanço tecnológico. Segurança da informação.

ABSTRACT

Cybercrimes, computer crimes or cybercrime, the names of Internet crimes over the years, have become popular with the advancement of the connection by society, which is due to the various forms of interaction between individuals that have emerged over the years. As well as the emergence of new forms of interactions between users, new forms of crime have emerged in similar proportions. The primary objective of this work is to make clear the uncontrolled growth of this type of crime, provided by our modern, fast and dynamic economy, enhanced by the advancement of technologies and the benefits of the digital age. Aiming to publicize and fulfill the role of social education, the growth of security incidents in the country is highlighted, showing that people and organizations have learned about the risks they face. Finally, the threats of the digital world were analyzed, in which people and organizations need to establish secure connections and interact in commercial and institutional relationships, applying good security practices, with the presentation of specific legislation that became necessary for the regulation and punishment of cybercrimes.

Keywords: Cybercrimes. Civil Law of the Internet. General Data Protection Law. Technological progress. Information security.

SUMÁRIO

INTRODUÇÃO

As atividades ilegais realizadas pela Internet têm trazido enormes dificuldades práticas para punir os infratores, pois ainda são poucas as leis que podem representar as mesmas, portanto, há muita impunidade para a prática de crimes no campo virtual.

É importante destacar que a Lei nº 12.695 de 2014 (rebatizada de Marco Civil da Internet), juntamente com a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados) trouxeram um grande progresso relacionado ao uso da Internet no estabelecimento das responsabilidades e direitos dos usuários da Internet. Porém, infelizmente, no campo da tecnologia da informação, o aumento anormal da criminalidade tem superado a prevenção e a evolução legislativa na fiscalização desta questão. Portanto, no Brasil, a legislação penal vigente é aplicada por meio de um arcabouço legal, como exemplo, no caso de roubo de valores em contas bancárias e preconceito e discriminação, a lei não regula especificamente esses crimes na rede de computadores, assim como danos à reputação e ameaças na maioria dos casos. Portanto, mesmo com o desenvolvimento do ordenamento jurídico, ainda é necessário prever regulamentação especial sobre diversos atos ilícitos nas mídias virtuais, a fim de reduzir as lacunas na legislação relacionada aos crimes virtuais.

O surgimento de novas tipificações penais, torna de suma importância as alterações na legislação com o desenvolvimento de novas tecnologias pois, os criminosos estão presentes em todo o globo de crimes na sociedade da informação, com a finalidade da aplicação efetiva das regras penais. Diante dessa realidade factual, as pesquisas sobre o tema tornam-se mais relevantes, pois se entende em que condições a legislação brasileira está preparada para lidar com tais crimes.

Além disso, é necessário analisar como conduzir as investigações criminais, diante a possibilidade do anonimato que acaba tornando mais difícil a identificação dos infratores e o fornecimento de provas e julgamentos nesses casos. O objetivo principal se baseia no conhecimento perante o que é crime virtual e suas características, que ajudam a entender o assunto e desenvolver métodos para melhorar a detecção e as evidências.

O crime virtual pode ter uma definição puramente virtual, mas seu impacto é fácil de entender no chamado “mundo real”, atualmente, as duas definições não podem ser separadas porque o crime virtual tem um grande impacto no cotidiano da sociedade.

Os crimes de reputação na Internet têm sido combatidos por leis existentes (como a própria Constituição, o Código Civil e o Código Penal), enquanto o Código Judiciário vem se ajustando para lidar com os crimes digitais e faltam crimes ante eletrônicos. No caso de

legislação especial, os tribunais brasileiros enfrentam e punem internautas, vigaristas e hackers que usam a Internet como ferramenta criminosa.

Ademais, essa monografia visa identificar pontuar e especificar os crimes virtuais que mais fazem vítimas no Brasil e mostrar as formas de punições a se aplicar, com base nas dificuldades do ordenamento jurídico sobre a questão e os caminhos a serem percorridos para uma internet mais segura com leis positivadas e uma legislação eficiente. A especificação e análise dos crimes na rede mundial de computadores, que se expandiram e infelizmente está cada dia mais presente no cotidiano dos mais variados usuários da internet no Brasil é necessária para averiguação em meios informáticos como base de dados de empresas, pessoas físicas, instituições de cunho financeiro, sistemas de informação e comunicação dos poderes judiciário, executivo e legislativo.

A análise do tema em vista dos cibercrimes, se sucedeu através da leitura de dados técnicos e fichamento produções textuais sobre a temática, e de pesquisas jurisprudenciais e referências bibliográficas das matérias.

O método utilizado é a leitura das obras realizadas na área, a própria investigação jurídica sobre o crime cibernético em face da 12.737 e demais legislações vigentes, juntamente com a recuperação bibliográfica de livros, artigos e periódicos jurídicos sobre o assunto são realizadas em etapas. Em termos de explicações gerais de fenômenos menos abstratos, nas investigações específicas para fins mais restritivos foram usados momentos históricos que incluem a investigação de eventos, processos e sistemas passados e a verificação de seu impacto na sociedade e nas mudanças tecnológicas dessa forma, será estudada a forma de influência e como o desenvolvimento tecnológico interfere no comportamento social.

CAPÍTULO 1 – INTERNET E SEGURANÇA DA INFORMAÇÃO

1.1 Internet e a Web 2.0

A conexão à internet inicializou na fase da Guerra Fria. A aplicabilidade dominante era a transferência de comunicações e seu emprego era exclusivamente militar. Com o passar dos anos, a tecnologia evoluiu. Dessa maneira, a internet passou a fazer parte da rotina de todos na sociedade. Há infinitas finalidades possibilitadas pela internet e as trocas de informações são eficientes apesar da distância entre os usuários.

> A internet é, portanto, uma rede mundial de computadores ou terminais ligados entre si, que tem em comum um conjunto de protocolos e serviços, de uma forma que os usuários conectados possam usufruir de serviços de informação e comunicação de alcance mundial através de linhas telefônicas comuns, linhas de comunicação privadas, satélites e outros serviços de telecomunicações. (MORAIS; LIMA; FRANCO, 2012, p. 42).

A rede mundial de computadores interligados, desde seu advento na década de 1960, continua potencializando suas aplicações. Sua capacidade noutrora constituída meramente por textos, atualmente permite a integração de sons, imagens e vídeos em tempo real. Além disso, com habilidade de comunicação em via dupla, a internet ocupa cada vez mais espaço na vivência dos seres humanos, pois possibilita o uso tanto na esfera pessoal quanto na profissional, seja para o simples fato de trocar ideias ou até para a comercialização eletrônica.

A propósito, Winck (2012, p. 11) aduz: “há alguns anos a grande rede de computadores conhecida como internet era considerada apenas como um novo meio de comunicação, alcançando no decorrer dos últimos anos um novo patamar de necessidade social”.

Através das barreiras de espaço, pela rapidez, impessoalidade ou anonimato na troca de informações, a comunicação proporcionada pela internet fora do ambiente virtual é inimaginável. Este avanço tecnológico trouxe muitos benefícios para o dia a dia das pessoas, o que levou à chamada era da informação ou era digital, onde qualquer informação pode ser obtida com um único clique e qualquer produto ou serviço pode ser fornecido e contratado por qualquer indivíduo possuindo uma máquina com acesso à internet. No decorrer da realização desta pesquisa, torna-se possível averiguar que os benefícios gerados através destas soluções digitais são de grande valia para a sociedade.

Por outro lado, uma parcela alta da população ainda permanece fora dos contornos das atuais técnicas disponibilizadas, os motivos são desde não saber fazer uso da ferramenta ou até a impossibilidade de acesso a ela por falta de recursos necessários. Isto posto, percebe-se

porquanto em que os benefícios de desenvolver atividades corriqueiras a todos e a clareza de procurar o conhecimento, por meios dos mecanismos da era da informação não perpassam por todos da sociedade, expandindo as possibilidades de disparar, ainda mais, as desigualdades sociais, pois, como refere Winck (2012, p. 13), “possuir informação permite vantagens no mundo globalizado”.

Sendo assim, observando os benefícios da massiva utilização de máquinas conectadas à rede na sociedade moderna, a Organização das Nações Unidas (ONU),através de um comunicado considerou o acesso à internet como direito humano, no ano de 2011, com a intenção de oferecer esta conexão possível para toda a população, sem distinguir as classes econômica, raça, cor, religião não importando com alguma diferença. A ONU compreende que o corte ao acesso à internet, independentemente da justificativa e incluindo violação de direitos de propriedade intelectuais como motivo, "uma violação artigo 19, parágrafo 3 º, do Pacto Internacional sobre os Direitos Civis e Políticos".

O presente século se mostra como o século da chamada era digital, apesar que esta era de mudanças on-line, bem como considerado como era da informação e era virtual, tenha se iniciado um pouco tempo antes do século atual, é neste período em que as transmutações decorrentes dele estão sendo absorvidas pela sociedade. Constata-se que o público se movimenta em direção ao fortalecimento desta chamada sociedade da informação e, indubitavelmente, o acesso à internet foi um dos elementos que impulsionou esta nova era.

Neste sentido, George Leal Jamil e Jorge Tadeu de Ramos Neves (2010, p. 9) afirmam que “a rede internet é instrumento básico para a construção desse novo cenário de organizações e comunicações virtuais, por si só, preconizam a mudança que se institui na palavra de diversos autores sobre a revolução do momento atual”. Sendo assim, os avanços tecnológicos proporcionados pela utilização da internet no sistema capitalista ensejaram uma série de transformações da sociedade em seus diversos segmentos, sendo sentidas mudanças nas relações de comunicação e de consumo entre os indivíduos da família e do trabalho, do espaço público e do espaço privado. Como refere Manuel Castells (2003, p. 34) “a cultura dos produtores da internet moldou o meio”.

Ademais, é possível notar que as ofertas de utilidades na web aumentaram para todos os setores da sociedade e, em virtude disso, a internet está ocupando cada vez mais espaço na vida dos indivíduos. De simples meio de comunicação, ela passou a se apresentar como uma múltipla ferramenta. Na medida em que oferece uma infinidade de músicas, jogos, imagens, vídeos, notícias e leituras variadas, a internet se revela como forma de entretenimento. Paralelamente, a mesma ferramenta também se apresenta como prestadora de serviços bancários on-line,

cadastros em diversos órgãos públicos e privados, acesso aos serviços públicos, procura de emprego, compra de ingressos para várias festividades, reservas de hotel e demais locais necessários. Além disso, percebe-se que a internet vem aprimorando seus serviços também no comércio eletrônico no que tange a negócios, comercialização de bens, produtos e serviços, quanto aos serviços disponibilizados na web. Elisabeth Gomes (2002, p. 6), quando assessora da Presidência da Anatel, referiu:

> São diversos os serviços oferecidos aos cidadãos, como por exemplo, a obtenção de certidões e inscrições de concursos via Internet, requerimento de benefícios previdenciários, cartão bancário para recebimento de benefícios capilarizando a rede de pagamentos e suprimindo as filas, pagamento eletrônico de impostos, taxas e contribuições, consultas públicas sobre propostas de leis, decretos e atos normativos, o cartão do Sistema Único de Saúde que condensará a memória da vida médica do usuário dos serviços, enfim, um vasto elenco de iniciativas e programas de governo eletrônico.

A expressão Web 2.0 foi utilizada originalmente por Tim O'Reilly enquanto participava de um conjunto de conferências sobre a temática, em São Francisco (EUA), proporcionadas pela companhia de comunicação MediaLive. Os debates eram direcionados para a função interativa dessa rede e a expressão se tornou rapidamente popular, também sendo nomeada como uma web social. De acordo com O'Reilly (2005), a Web 2.0:

> É uma plataforma na internet que abrange todos os dispositivos conectados [...] as aplicações [...] são aquelas que aproveitam o máximo as vantagens intrínsecas que essa plataforma oferece: fornecimento de software como um serviço continuamente atualizado que fica melhor quanto mais pessoas usá-lo, consumindo e ligando dados de várias fontes, incluindo os de usuários individuais, enquanto providencia os seus próprios dados e serviços de forma que permitem os outros indexarem, criando efeitos de rede através de uma "arquitetura de participação". (tradução nossa)

A Web 2.0, parte da Web 1.0 para oferecer ricas experiências de usuário. Diante disso, a Web 2.0 têm seus princípios baseados na participação de seus usuários, sendo, portanto, uma plataforma interativa que proporciona "aos mais variados públicos [...] o poder de publicar conteúdo digital utilizando recursos como e-mail [...] blogs [...], microblogs [...], podcasting [...], redes sociais [...], e wikis [...]" (ALVES, 2011, p. 97).

As características primordiais da Web 2.0 acompanham as mesmas da Web 1.0, motivo pelo qual vale discutir e diferenciar ambas. A última apresenta recursos estáticos, as informações disponibilizadas servem apenas para leitura, ocorrendo pouca interação com os usuários, pois os aplicativos são fechados para alteração.

Sobre a Web 2.0, por seu turno, explica Maness (2007, p. 44), “o termo é agora amplamente usado e interpretativo, mas a Web 2.0, essencialmente, não é uma Web de publicação textual, mas uma Web de comunicação multisensitiva”. A Web 2.0 apresenta caráter colaborativo e opera como uma matriz de diálogos, não uma coleção de monólogos. Ela é uma Web centrada no usuário.

Noutras palavras, na Web 1.0 o usuário era um mero espectador, enquanto na Web 2.0 ele passou a ser o mediador de conteúdo ao criar, modificar e compartilhar informações. De acordo com Machado (2010, p. 23), “na web 2.0 o objetivo principal é a construção de conteúdo, ou seja, todo usuário pode contribuir para o desenvolvimento e expansão da internet, criando e editando o conteúdo de forma coletiva”.

Dentro dessa nova realidade de uma usualidade, que autoriza os clientes corroborem com o ambiente tecnológico, efetuando a participação e a subdivisão de informações, entende-se também a importância de reforçar como o uso da web 2.0 se tornou mais simples, proporcionando uma melhor experiência com o meio tecnológico, oferecendo uma grande pluralidade de programas e plataformas de entretenimento, transformando a internet um ambiente mais inovador e intuitivo planejado para evoluções na forma de aprender.

Dessa forma, a Web 2.0 está em constante evolução e deixando seu escopo com um maior apelo social, favorecendo a interligação e a cooperação com seus utilizadores, considerando que no passado a web se organizava através de páginas que posicionavam toda a sua estrutura online, de forma fixa, não oferecendo alternativas de interatividade aos usuários. Dessa forma, existe chance de gerar uma ligação, através das sociedades de usuários com necessidades no mesmo âmbito, como decorrência da utilização da plataforma mais comunicativa e dinâmica a internet se descreveu a Web 2.0, da seguinte forma: “[...] ambiente social e acessível a todos os utilizadores, um espaço onde cada um seleciona e controla a informação de acordo com as suas necessidades e interesses” (COUTINHO; BOTTENTUIT JUNIOR, 2007, p. 200).

Portanto a premissa desta pesquisa não está no modelo estático da chamada Web 1.0, mas sim na Web 2.0 e, especialmente, nos princípios usados com a intenção de suprir demandas da sociedade em rede, olhando a parte social e colaborativa dos utilizadores que conglomeram criadores e usuários de informação nesse mundo conectado.

1.2 Segurança da Informação

O indivíduo para que tenha garantida a liberdade de atuação no mundo virtual tem que ter seus direitos fundamentais atendidos, a fim de preservar os princípios inerentes à pessoa humana, como disciplina o texto constitucional brasileiro. Ademais, dentre os direitos fundamentais resguardados no ambiente digital o direito a proteção de dados pessoais é um dos mais significativos da humanidade na contemporaneidade, como destaca Fortes (2016).

O direito à proteção dos dados pessoais na internet engloba uma gama de fundamentos e princípios que são indispensáveis para o desenvolvimento da personalidade do indivíduo, tanto na internet quanto fora dela, conforme se depreende dos ensinos de Rodotà (2008).

Rodotá (2008) trata a proteção de dados como uma expressão de liberdade e dignidade pessoal, assim não é admissível que o uso dos dados transforme a pessoa em um objeto em vigilância constante. O autor relata que progresso da tecnologia e da relação dela com a vida das pessoas têm transformado os indivíduos em cidadãos da rede, que em um contato constante com o ambiente digital possuem seus hábitos, movimento e contatos perfilados, o que impacta de modo significativo na autonomia dos indivíduos, indo de encontro com a natureza da proteção de dados pessoais na qualidade de direito fundamental.

Assim, para que haja a liberdade para os indivíduos conviverem com tranquilidade no ambiente virtual é necessário a garantia da proteção de seus dados pessoais, obrigando os sites e aplicativos a realizarem o uso ético das informações, bem como, cumprir com o tratamento adequado. Cabe ao direito, por meio da atuação do Estado, garantir que a sejam cumpridas as diretrizes para efetivação do direito de guarda das informações de cunho pessoal (FORTES, 2016).

Segundo o Núcleo de Informação e Coordenação do Ponto BR (NIC.Br), a segurança da informação desenvolve duas divisões: a segurança digital e a segurança cibernética. Esse assunto está se tornando cada vez mais relevante, em decorrência dos frequentes riscos do mundo on-line que vêm gerando preocupações em organizações e escritórios, tomado o vasto número de ataques virtuais organizados por criminosos cibernéticos. A segurança da informação tem o objetivo de assegurar que as informações, digitais e físicas, fiquem protegidas contra possíveis ataques externos. Como consequência desse fator, se torna mais fácil considerar que a segurança digital cuida dos dados digitais, enquanto a segurança cibernética protege contra os ataques cibernéticos.

A internet é uma ferramenta de informação e comunicação que permite a troca de informações em geral, por meio da qual as pessoas possam exercer abertamente sua liberdade de expressão e que, em face disso, dá espaço para que os indivíduos venham a cometer

atividades delituosas. Além disso, como é uma ferramenta relativamente recente, já que faz poucos anos que a internet se tornou amplamente disponível e que em algumas regiões ainda não existe acesso irrestrito a ela, as leis ainda vêm sendo desenvolvidas e alteradas para que possam abranger essas ocorrências, inexistentes até então.

Observando-se pelo prisma jurídico, a internet pode ser entendida como uma rede transnacional de computadores interligados, com a finalidade de trocar informações diversas e na qual o usuário ingressa, por vários meios, mas sempre acaba por realizar dato jurídico, gerando consequências inúmeras nas mais variadas localidades (ROSA, 2005, p. 35-36).

Contudo, Doneda (2011) relata que a partir da leitura das garantias constitucionais verifica-se que não abrange a complexidade do fenômeno do desenvolvimento tecnológico, por conseguinte, a legislação infraconstitucional aliada a evolução da internet, passou a dar a devida preocupação à proteção dos dados pessoais, com a adição de dispositivos em leis esparsas para garantir ao titular dos dados pessoais o controle sobre as informações contidas nos bancos de dados físicos e virtuais, tema que será abordado com mais ênfase mais adiante.

Em 14 de agosto de 2018, foi sancionada a Lei nº 13.709, a Lei Geral de Proteção de Dados Pessoais, diploma nacional voltado exclusivamente para a regulação da garantia de guarda das informações pessoais. A lei é alicerçada pelos fundamentos já mencionados, seguindo os princípios da boa-fé, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas, conforme disciplina o seu artigo 6º, o qual será tratado em momento oportuno a seguir (BRASIL, 2018).

Em síntese, o direito a proteção de dados pessoais é direito fundamental a ser garantido não só em um mundo físico, mas também no ciberespaço, pois na chamada sociedade da informação a internet está ocupada por pessoas, empresas, instituições, organizações e o próprio Estado, e os direitos fundamentais tem um papel relevante a ser desempenhado nesse ambiente, dando a devida proteção a dignidade da pessoa usuária da rede (FORTES, 2016; DONEDA, 2011)

1.3 Vulnerabilidade do usuário na internet

A internet vem evoluindo de forma exponencial, nunca houve na história da humanidade uma forma de comunicação que se desenvolveu tão rapidamente, afetando da forma de ler à forma de entreter. A web coloca toda a vivência do mundo para dentro de nosso lar, profissão e formação acadêmica. A revolução digital é considerada a mobilização para inserir no

cotidiano dos indivíduos as evoluções tecnológicas e as ferramentas que fazem uso de criações inovadoras, alterando o modelo de como o dia a dia evolui.

A difusão das máquinas de acesso à rede pelo fato da redução de custos e o crescimento da disponibilidade (aumento da celeridade de conexão, ferramentas mais robustas e protocolos desenvolvidos de maneira mais simples) corroboram para os crescimentos de usuários. Dia após dia mais indivíduos no globo possuem conexão com a internet e, dessa maneira, a web modifica a rotina da sociedade, posto que as situações cotidianas tendem a ser informatizadas e as possibilidades são imensas.

Todavia, ainda que as vantagens na sociedade cibernética sejam inegáveis, existe um receio pelo fato do aumento dos crimes na internet e, mesmo com novas leis aumentando o rol de algumas penas aos desregramentos e crimes cibernéticos, até então não estamos habilitados para evitá-los por completo. “O avanço e a polarização da tecnologia aliada à informática fizeram com que surgissem novos hábitos e, com eles novos valores. Na medida em que tais valores adquirem relevância social e econômica, surgem também problemas quanto a sua preservação” (SYDOW, 2015, p. 21).

Uma das maiores vantagens que a internet trouxe é a capacidade de abranger variados conteúdos profissionais e de entretenimento no mesmo ambiente, fotografias, músicas, investimentos bancários, arquivos, planilhas, se acessa tudo através da mesma máquina ou dispositivo móvel, em qualquer lugar que o usuário esteja. Irrefutavelmente, nota-se um progresso que fomenta a vivência das pessoas na era atual.

Nos dias atuais, programas estão sendo desenvolvidos para englobar toda a rotina de um utilizador da rede. Aplicativos também estão sendo criados para propor os melhores locais para se fazer uma refeição, para fazer publicações instantaneamente o que se faz no cotidiano, para atendimentos médicos, para coordenarem as ocupações de cunho pessoal ou profissional de cada pessoa. São infinitas as vantagens oferecidas no mundo da internet, como explana Luiz Ribeiro (2010):

> De um simples site a um mega portal de conteúdo há muitas coisas parecidas que em pouquíssimos ambientes pode-se encontrar. Da mesma forma, blogs, sites, portais, sistemas, etc., são parte da mesma matéria-prima e por mais que tenham propósitos e fins diferentes, acabam por convergir e fazendo uma mistura que muitos procuram entender (RIBEIRO, 2010).

Considera-se que esta evolução acaba por trazer funções diferenciadas e muitas melhorias, por outro lado, novos perigos nas áreas tecnológicas obrigam que as mais variadas esferas da comunidade passem a ficar vigilantes a potenciais transgressões e infrações contra a

ética tais como discriminação racial, pornografia infantil, propagação de vírus, crimes contra a honra, extremismo, invasões a bancos de dados, comercio ilícito de drogas e remédios controlados e estelionatos comerciais.

Ao analisar dados de ataques reportados ao do Centro de Estudos, Respostas e Tratamento de Incidentes da Segurança Nacional (CERT.br), conseguimos captar levantamentos de ações executadas pela internet que causam uma sequência variada de crimes, sendo exemplos as fraudes e ações maliciosas com sistemas de usurpação de dados, como Scan, worn, DoS.

Com a crescente acesso de pessoas na rede mundial de computadores, um número ilimitado de informações começara a ser propagadas. O usuário utiliza a internet como meio de acesso a diversificados tipos de informações e uma densa gama de atividades que podem ser realizadas. Entretanto, as informações disponibilizadas com ou sem autorização podem trazer penalidades se distribuídas de maneira ilícita.

O Código Civil garante a proteção da privacidade como também 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: “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”.

Ademais, é dever do Estado a garantia ao cidadão do direito de proteção a identidade, consequentemente, que seus dados disponibilizados sejam usados somente para determinados objeto específicos. Outrossim informações pessoais de qualquer pessoa natural ou jurídica, não devem ser tratadas como mercadorias, ou seja, desconsiderando seus aspectos como um todo.

Diante a gama de possibilidades que a tecnologia pode trazer, as pessoas passam a depender de empresas de diversificados softwares, conectando ambos a rede mundial de computadores, elevando ainda mais as informações e os modelos tanto estratégicos quanto pessoas de servidores de empresas, aumentando a necessidade diante o monitoramento da segurança de informação. Conquanto, o usuário acaba ficando vulnerável a práticas de crimes no meio informacional.

O Código Penal não tipifica de forma específica o crime de espionagem eletrônica, embora a conduta possa ser compreendida nos artigos 154 e 154-A:

> Art. 154. 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.

> Art. 154-A. 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.

De acordo com a Consolidação das Leis Trabalhistas em seu artigo 482, "g" que o funcionário que praticar a conduta de espionagem poderá ter seu contrato rescindido: "Constituem justa causa para rescisão do contrato de trabalho pelo empregador: [...] g) violação de segredo da empresa". Outrossim, em ambientes de trabalho é necessário que se tenha mais segurança diante os dados e aplicações da empresa, pois as mesmas estão voláteis a ameaças internas, que acabam se tornando mais difíceis de serem identificadas por serem feitas por usuário legítimo, que não possibilita rastreamento. Patrícia Peck (2010, p. 385) descreve:

> 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 móveis e bloqueio de portas USB; criação de canal de denúncia; garantia de acesso somente a quem é necessário; realização de testes de vulnerabilidade.

Com o advento do uso da tecnologia voltado para a venda, jogos, relacionamentos e trabalhos a internet possibilita interação em tempo real para seus usuários, além da possibilidade de lazer e acesso à educação. A fraude virtual, por exemplo, é conduta advinda da invasão, modificação ou alteração diante sistemas de processamento, que são frequentemente usados.

O CERT-BR (Centro de estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil) em seu anuário sobre crimes eletrônicos, descreve que fraude eletrônica se dá por mensagem não solicitada a fim de se passar por instituição conhecida ou ainda a mensagens que induzem o usuário a instalar de códigos de origem duvidosa.

As fraudes virtuais são classificadas em duas vertentes: externas, nas quais quem comete a fraude não tem vínculo direto com o local a ser fraudado e a fraude interna que é cometida por infrator imerso no local a ser fraudado, seja ele um morador ou empregado ou mesmo um terceiro que esteja prestando serviço ou de passagem pelo local.

Nos crimes de fraude virtual, o usuário da rede é induzido a fornecer dados pessoais e/ou financeiros, através de fraudadores que através de redes sociais conseguem convencer e enganar usuários.

1.4 Padrões de comportamento do usuário na internet

Diversas mudanças na humanidade foram causadas por conta da internet, dentre elas os conceitos reguladores responsáveis por diferenciar o público do privado, como também outros hábitos inerentes para uma convivência harmoniosa, vem ganhando outros significados e limites. Isso ocorre pelo fato que, através da conexão pela rede e na falta da convivência humana pessoalmente, a necessidade por ser reconhecido e conhecer, acaba por influenciar a seletividade na questão sobre como pessoas alheias terão de entendimento sobre o eu.

A interatividade acaba caracterizando uma maneira de alimentar convívios com privilégios ou prestígios, dentro de uma sociedade com grande relevância a nível global como a internet. É possível observar a quebra de barreiras, por exemplo a realidade que ficava por trás dos palcos e câmeras, se tornaram visíveis aos usuários da rede, hoje conseguem acessar e divulgar mídias de áudio e vídeo que antes ficavam restritos aos bastidores.

Em termos de compartilhamento e acessos a postagens, a rede mundial de computadores é conhecida por ser um ambiente com alto grau de democracia. Nenhum usuário da web necessita solicitar autorização a instituições ou órgãos tanto governamentais ou empresas privadas, para expor opiniões ou qualquer outro pensamento que ele achar pertinente. (CULTURA DIGITAL, 2010). Não havendo cerceamentos para acessar as mídias digitais e postagens, seja a qualquer hora e idade, os usuários da internet a fazem o uso dentre seus próprios anseios preceitos como humildade, cortesia, cautela e outros gestos considerados relevantes em público são invalidados sem coibição imediata. Mesmo que essa situação existia, é simples ignorar o fato apenas desativando o acesso à rede. O equívoco é que nosso acesso e publicações de conteúdo na internet sem sermos notados, avaliados ou mesmo identificados está relacionado à impressão de que estamos livres de culpa, o que pode gerar comportamentos irresponsáveis, inconsciente ou mesmo criminosos.

Fazendo a comparação de atitudes em situações reais e virtuais, entende-se que há duas realidades presentes: na situação presencial existe uma atitude complacente e prudente, todavia no mundo digital há uma alteração nas pudores no que se está expondo e postando, sendo uma espécie de preocupação com sua própria imagem, com a imagem alheia, com as interações acessadas e expostas.

A problemática relatada, tem gerado usuários que não sabem proceder no ambiente virtual, de forma que não produza problemáticas a si próprio, como ultra exposição de dados pessoais e ocorrências de “hates”. Para que haja uma melhora do convívio do usuário com o meio virtual e este se torne um indivíduo com boas maneiras e tenha uma experiência positiva com a web, é necessário que ocorra uma ruptura de barreiras socioeconômicas, que não seja de

uma forma abrupta ou a curto prazo, pois se tratando de avanços socias, as alterações ocorrem de maneiras graduais.

Segundo as considerações de Wouters (2009), para compreendermos as mudanças comportamentais, criam se debates e entendimentos sobre as etapas do comportamento de Nobert Elias (teoria Elisiana), entende se o surgimento de um fato social, classificado pelo autor como descontrole controlado. As condutas se dividem em três fases, que explicitam como o indivíduo se relaciona com o tempo.

A forma como o indivíduo expressa o comportamento dos seus ensejos naturais, faltando a autorregulação que rotule o que é considerado aceitável ou reprovável pela sociedade, estimula a atender imediatamente as vontades próprias, essa é a classificação da chamada primeira natureza.

Portanto a segunda natureza, perpassa pelo autocontrole, intrínseca da própria pessoa, considerando sua experiência e vivência dentro dos padrões comportamentais, as condutas são exclusivamente executadas depois de uma crítica em relação as regras sociais quanto a etiqueta e pudor.

Como disciplinador da sua conduta, existe o medo de ser exposto, ser julgado ou atacado por conta de seus pensamentos ou ações, portanto em diversas situações, por conta do auto regramento, o indivíduo se encontra com receio de demonstrar suas vontades e o estilo de vida em que está incorporado. O autocontrole automático de um hábito que, dentro de certos limites, funciona também quando a pessoa está sozinha. Ao contrário, o controle dos instintos era inicialmente imposto apenas quando na companhia de outras pessoas, isto é, mais conscientemente por razões sociais. (ELIAS, 1994, p. 142-143).

Com o avanço da civilização a vida dos seres humanos fica cada vez mais dividida entre uma esfera íntima e uma pública, entre comportamento secreto e público. E esta divisão é aceita como tão natural, torna-se um hábito tão compulsivo, que mal é percebida pela consciência. (ELIAS, 1994b, p. 188). Com o estreitamento das relações entre os indivíduos e as possibilidades de trocas socioculturais entre espaços, culturas e aprendizagens diferenciadas, os comportamentos foram flexibilizados diante 34 dos diferentes níveis de tolerância aos impulsos emocionais das sociedades e gerações.

Na sociedade global do século XXI, a internet não é uma simples tecnologia de comunicação, mas o epicentro de muitas áreas da atividade social, econômica e política, (BOTTENTUIT JÚNIOR; COUTINHO, 2007). Esse frenético avanço das Tecnologias de Informação e Comunicação (TICs) trouxe para a interação do ser humano com o ser humano e

do ser humano com diferentes serviços, a urgente necessidade de se aprender na prática como reorganizar e ampliar as atividades do dia a dia por meio da praticidade da internet.

Diante da demanda, aprendemos a interagir com o computador e internet de maneira informal, a partir da curiosidade e colaboração de quem sabe um pouco mais. Aos poucos ou em explosões do modismo, transferimos para o mundo virtual muitas das nossas atividades reais e até reinventamos tantas outras, deste modo as possibilidades da internet imitam, reproduzem e dão continuidade aos fenômenos da vida real, o resultado é um ambiente organizado como mais um espaço de interatividade sociocultural.

O uso das tecnologias geralmente rompe com o que até então estava estagnado, esse rompante pode caracterizar-se com avanços, retrocessos ou estagnações, conforme os níveis de assimilação e adaptação das sociedades. Com o fenômeno da internet não seria diferente, assim como aprendemos a lidar de modo consciente e seguro com o autoatendimento nos caixas eletrônicos dos bancos, também precisamos nos adaptar e aprender a lidar com as facilidades e riscos de navegar pela internet, é necessário questionarmos sobre o modo como acessamos, disponibilizamos e usamos as informações e as ferramentas da rede.

Compomos por meio de sites, redes sociais, fotos, vídeos e outras linguagens esse mundo sem fronteiras, livre e sem medida, no qual a ânsia pelo acesso e atualização, de tudo e de todos, ofusca a preocupação com a dimensão e consequência do que é feito quando se está na rede. Nosso interesse pelas mídias e as relações dos indivíduos com elas e a partir delas, motivou-nos a pesquisar desta vez as dinâmicas interativas entre pessoas, bens e serviços organizadas por meio da internet.

Diante das potencialidades que esse meio nos oferece, observamos a crescente necessidade de que haja uma certa formação para o uso, pois por parte dos indivíduos há uma ausência de informação e formação e se encontram em rede mundial conectada, repleta de usuários com boas e más intenções, que tem comprometido a navegação a ponto de expor o internauta a diferentes riscos. Ou seja, acesso a conteúdos inapropriados à idade (e até mesmo ao discernimento), envolvimento consciente ou inconsciente em ações ilegais; exposição a golpes, fraudes, ameaças, assédios entre outros atos que perturbam a segurança ou a integridade pessoal de si mesmo ou do outro.

A ausência de uma formação ou de acesso a um guia para o acesso à internet resulta muitas vezes em constrangimentos sociais, em um ou vários ambientes da internet, como também este usuário se torna um alvo, em meio aos vários modos de golpes e formas de estelionato que são recorrentes na rede mundial de computadores.

Frente à positividade da internet nas interações humanas, é que propomos uma mudança comportamental para melhor utilizarmos essa tecnologia sem que estejamos expostos a experiências ruins e perigosas, e que a partir disso possamos cada vez mais utilizar de seus aspectos positivos, como colaboração em rede, entretenimento, aprendizagens, etc. Sendo assim as considerações trazidas ao longo da pesquisa não são para negativar ou invalidar a importância das iniciativas de ONGs, empresas e órgãos públicos que se propõem em informar e formar a população acerca da necessidade de se acessar a internet de maneira segura e consciente.

CAPÍTULO 2 – N OÇÕES INICIAIS SOBRE OS CRIMES ELETRÔNICOS

2.1 Conceitos de crimes eletrônicos

Com a disseminação do acesso à internet, a política, o meio jurídico e social, passaram também por mudanças significativas. Ademais, acabou sendo exigido também o aperfeiçoamento do Direito, para que o mesmo possa compreender e se moldar diante á era digital, impedindo que a população se torne meio de controle estatal, mas que também garanta privacidade e intimidade.

Na concepção Ramalho Terceiro (2002), é descrito que:

> Os crimes perpetrados neste ambiente se caracterizam pela ausência física do agente ativo; por isso, ficaram usualmente definidos como sendo crimes virtuais. Ou seja, os delitos praticados por meio da Internet são denominados de crimes virtuais, devido à ausência física de seus autores e seus asseclas.

O entendimento de Augusto Rossini (2004, p. 110) descreve:

> O conceito de ‘delito informático’ poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade e a confidencialidade.

Entretanto, a comodidade e o conforto, que é possibilitado pelo acesso à internet, como para compras e acesso a diversificados sites, acabam permitindo a circulação de dados de usuários em diversas plataformas, que por diversas vezes são expostas para criminosos. A Lei 12.737/2012 exige que se mantenha sem alteração dispositivos informáticos, por meio do tipo penal previsto no Decreto-Lei 2.848/40, que descreve penalidades diante ataques a liberdade individual.

> Art. 154-A. 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: Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.

Outrossim, a Constituição Federal de 1988 no seu artigo 5º, X, descreve que se é garantido a proteção da privacidade, promovendo ao cidadão direito a reparação se tiver a mesma violada.

> 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.

No contexto jurídico, é necessário que se preserve a privacidade e a liberdade do indivíduo como um todo, e principalmente dados ou quaisquer outras informações que circulem na internet. A rede de computadores é propícia para áreas de atividade social, econômica e política, sendo o ponto de "encontro" da maioria da sociedade moderna, por meio de mensagens de texto, ligações de vídeos e trocas de e-mails, por exemplo.

Entretanto, o direito à privacidade e o direito à liberdade de expressão são expressões antagônicas quando dispostas por usuários de redes sociais, que promovem por diversas vezes difamação, ofensa a honra e violação de privacidade por meio de comentários, vídeos e outros meios postados na internet. Portanto, acaba sendo necessário uma nova análise diante condutas praticadas por usuários nas redes, para que seja garantida de maneira efetiva a dignidade e interesses diante personalidade.

De acordo com Rossini (2002), existem duas maneiras de delitos na internet. Os "delitos informáticos puros" são aqueles que o sujeito visa especificamente atingir o sistema informático em todas as suas formas. Já os "delitos informáticos mistos" são aqueles praticados quando o computador se torna uma mera ferramenta para a prática de ofensas e ataques a outros bens jurídicos além do sistema informatizado. Em vista dos delitos praticados pela internet, projetos de lei são propostos com frequência como meio de um maior controle sobre a liberdade da população.

No Brasil, os crimes virtuais foram conhecidos no mundo jurídico como "delitos informáticos", termo já utilizado em países como a Espanha. Certa nomeação traz derivação da ideia de preservação e proteção de bens jurídicos, sendo a rede ou informações contidas na mesma.

Atualmente, crimes de ameaças podem acontecer por meio de e-mails ou comentários em sites de relacionamentos. O mesmo é tipificado pelo artigo 147 do Código Penal, ou seja, a tecnologia se tornou apenas um novo meio para que seja praticado crimes já previstos em lei.

A fraude bancária também se tornou um dos crimes que começaram a ocorrer por meio de apenas um clique. A comodidade de gerenciar contas bancárias ou fazer compras por meio de tela de computadores e smartphones, fizeram com que dados sigilosos se tornassem vulneráveis a ataques cibernéticos. O cavalo de tróia, por exemplo, é instalado no computador para que possa fazer captação de maneira indevida de dados com a intenção de subtrair patrimônio de determinada vítima. Organizações criminosas que praticam tal ato podem ser enquadrados em crimes como interceptação telemática ilegal, descrito no artigo 10 da Lei 9.296/96, e violação de sigilo bancário, previsto punição no artigo 10 da Lei Complementar 105/2001. Ademais, crimes como furto qualificado mediante fraude e formação de quadrilha também podem ser dispositivos penais usados dependendo da maneira em que o crime foi praticado.

Jurisprudências brasileiras já possuem entendimento diante a condenação de empresas provedoras de conteúdo, como facebook e instagram, para punição diante usuários que apresentam conteúdos que infrinjam e ofendam outrem. Ademais, é inviável que se obrigue provedores a fazerem análises prévias e fiscalização diante o que cada usuário posta nas redes, mas deve ser facilitado para que a pessoa ofendida possa informar sobre a prática de atos sem que precise de ordem judicial.

Entretanto, a Constituição Federal de 1988 no artigo 5º, IX, proíbe qualquer espécie de censura, vedando todo procedimento que impeça a livre circulação de manifestação de ideias diante os diversos contextos da sociedade, porém, existem limites para o exercício de tal liberdade de expressão.

A Convenção de Budapeste, ou Convenção sobre Cibercrime, é o tratado internacional que dispões sobre crimes que são cometidos no meio cibernético. A mesma foi proposta pelo Conselho Europeu, e entrou em vigor em julho de 2004, com adesão de cerca de 30 países, inclusive os Estados Unidos que abriga o Google, o maior provedor de pesquisa na rede. É destacado a necessidade do impedimento de atos praticados contra a confidencialidade, integridade e disponibilidade dos sistemas informáticos e redes, e também a utilização por meio de fraudes de dados, assegurando que crimes desse modelo sejam incriminados com combate eficaz de tais infrações, tanto em nível nacional quanto internacional e uma cooperação entre os países para respostas rápidas e eficientes.

Contudo, o Brasil não se tornou signatário de tal convenção, mas possui disposições incorporados na legislação como pornografia infantil, cuja Lei 11.829/08 alterou a Lei 8.069/90 (ECA) nos artigos 240/241 e 241-A, inserindo condutas relacionadas à prática de pedofilia na internet.

A Lei 10.447/02 dispões também sofre infrações penais de repercussão interestadual ou internacional que exigem repressão, como disposto no inciso I do Capítulo 1º do artigo 144 da Constituição. Ademais, se têm a Lei 9.296/96 que dispõe sobre a interceptação do fluxo de comunicações nos sistemas informáticos e telemáticos, já previsto no artigo 21 da Convenção de Budapeste.

2.2 *Modus Operandi* dos crimes eletrônicos

Os crimes virtuais são atitudes ilícitas cometidas por indivíduos que se aproveitam das brechas dos sistemas digitais, e da fragilidade dos usuários leigos, para praticarem suas fraudes, podendo ser feitas através de dispositivos como o celular, tablet, notebook ou computador.

Há ainda quem ousa em aplicar golpes em departamentos públicos ou grandes empresas, nas palavras de Frederico Cattani, advogado criminalista, professor e especializado em crimes econômicos, "ter um plano para casos de ataque cibernético é igual a manter treinamentos para caso de incêndio", e expõe ainda que:

> Os agentes e firmas que lidam com matérias sensíveis ao empresariado e com impacto no mercado econômico são alvos recorrentes desses crimes e, por isso, estão investindo cada vez mais em profissionais e sistemas para manter suas bases de dados seguras. Trata-se de uma política interna de planejamento contra os crimes virtuais. Deve-se ter em mente que essa criminalidade está muito à frente das regras penais atuais, e a velocidade de uma investigação policial não acompanha a contenção de prejuízos em um cenário de perda ou sequestro de informações. (CATTANI, 2018)

Diferente dos outros crimes, as infrações cometidas em meios virtuais são executadas por alguém que contém habilidades e experiência tecnológica em aparelhos eletrônicos que conectam à internet, se proteger destes crimes não é fácil, porém há algumas ações de segurança que podem ajudar, como evitar fazer downloads de sites suspeitos ou desconhecidos, verificar com cautela a genuinidade de e-mails, principalmente de remetentes desconhecidos, jamais fornecer dados, logins e senhas.

Fabrizio Rosa (2002, p. 53) descreve os crimes de informática e como os mesmos podem acontecer:

> A conduta atente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar; 2. O 'Crime de Informática' é todo aquele procedimento que atenta contra os

> dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão; 3. Assim, o 'Crime de Informática' pressupõe does elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador, utilizando-se software e hardware, para perpetra-los; 4. A expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável, contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão; 5. Nos crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, etc.

Segundo a pesquisa da Norton Cyber Security Insights Report 2017, divulgado em 2018 pela Núcleo de Informação e Coordenação do Ponto BR (NIC.Br) listou o Brasil como o país com o segundo maior número de casos de crimes cibernéticos, perdendo apenas para a China.

Em 2017, aproximadamente 62 milhões de brasileiros foram afetados por alguns crimes cibernéticos. Os usuários de smartphones e aplicativos WhatsApp são os maiores alvos dos cibe criminosos. Phishing é a prática mais comum usada por golpistas e inclui o envio de conversas ou mensagens falsas com links fraudulentos. Por exemplo, quando esse link é aberto, os dados do usuário podem ser roubados ou apontar para uma loja online falsa. Sergio Marcos Roque (2007, p. 25), dá o conceito de crimes virtuais da seguinte forma "toda conduta, definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material".

Quanto à forma de autuação do agente, Monteiro Neto (2003) estabelece algumas explicações como a fraude por manipulação de um computador, a espionagem informática, a sabotagem informática, o furto do tempo, o acesso não autorizado e as ofensas tradicionais. Tais conceitos abrangem a modificação de dados dentro do sistema informático com o intuito de obter informações de maneira ilícita, obtenção de informações sigilosas por meio de sistema de informática, a sabotagem no meio informacional como maneira de modificação do sistema, o acesso a sistemas informáticos sem permissão para fins particulares, o acesso sem autorização para obtenção de informações sigilosas, podendo manipula-las, destruí-las ou altera-las, e por fim, a utilização do sistema para prática de atos ilícitos como a falsificação de documentos, respectivamente.

2.3 Meios telemáticos como instrumento

Anteriormente ao advento da internet, os serviços oferecidos por computadores eram possíveis de acesso apenas para aqueles que pudessem interagir de maneira física com o equipamento. A internet foi criada diante a necessidade do governo norte-americano em manter suas comunicações durante guerras ou ataques, o que acabou popularizando as redes de computadores e o desenvolvimento dos meios telemáticos. De acordo com Rita de Cássia Lopes da Silva (2003),

> O governo norte-americano queria desenvolver um sistema para que seus computadores militares pudessem trocar informações entre si, de uma base militar para a outra e que mesmo em caso de ataque nuclear os dados fossem preservados. Seria uma tecnologia de resistência. Foi assim que então a ARPANET, o antecessor da internet, um projeto iniciado pelo Departamento de Defesa dos Estados Unidos que realizou então a interconexão de computadores, através de um sistema conhecido como comutação de pacotes, que é um esquema de transmissão de dados em rede de computadores no qual as informações são divididas em pequenos "pacotes", que por sua vez contém trecho de dados, o endereço do destinatário e informações que permitiam a remontagem da mensagem original.

Telemática, ou teleinformática, é a conjugação da informática e dos meios de telecomunicação, ou seja, é a ciência que provê a infraestrutura necessária à troca de informações entre computadores e demais dispositivos informáticos, os quais geralmente interagem por meio de redes de telecomunicação (ROSSINI, 2004, p. 42-43).

O termo diz respeito não apenas à infraestrutura e aos protocolos necessários à comunicação entre computadores, mas também aos próprios serviços informáticos fornecidos por meio de redes de telecomunicações (HOUAISS, VILLAR, 2009, p. 1823), como por exemplo um serviço de e-mail interno de uma empresa ou um site acessível pela Internet.

Serviços que eram prestados de forma presencial, após a telemática e a informatização, passaram a ser disponíveis à distância, como os serviços bancários e o comércio eletrônico.

A interrupção de um serviço pode acorrer pelo aumento repentino de acessos legítimos, como grande acesso a sites que disponibilizam promoções, ou até mesmo, por ação criminosa, que acaba deixando o sistema lento ou interrompendo o mesmo. Conquanto, a interrupção de determinado serviço pode afetar o fluxo das informações, podendo acarretar prejuízos tanto na esfera econômica, quanto à vida e a integridade física, como em atendimentos médicos à distância.

2.3.1 Crimes de furto mediante fraude e estelionato eletrônico

O furto é um dos cibercrimes que ocorrem com frequência no meio virtual, no qual se obtém dados da vítima, senhas bancárias e informações sigilosas por meio de ato ilícito. O roubo de algo feito pela internet é incluído em sua maioria de acordo com o artigo 171 do Código Penal.

> **Estelionato**
> 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 um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis

Ademais, se o estelionato ocorrer contra idoso ou vulnerável, a pena aumenta 1/3 (um terço) ao dobro, de acordo com o parágrafo 4º do artigo 171.

De acordo com o artigo 155, do Código Penal Brasileiro, o furto mediante fraude poderá ter punição maior se o mesmo for feito por dispositivo eletrônico.

> Art. 155.
> § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo.
> § 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso:
> I – Aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional;
> II – Aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável.

No furto, a fraude é usada para burlar a vigilância da vítima, possibilitando que seja feita a subtração. Já no estelionato a fraude é utilizada como objeto de consentimento da vítima, que pode entregar voluntariamente, mesmo sem ter consciência do perigo, dados e informações ao cibercriminoso.

Decisão do Superior Tribunal de Justiça, exemplifica os crimes citados acima.

> CONFLITO DE COMPETÊNCIA. PROCESSUAL PENAL. CONTRATAÇÃO DE EMPRÉSTIMO BANCÁRIO E TRANSFERÊNCIA DE VALORES. FRAUDE ELETRÔNICA. AUSÊNCIA DEENTREGA VOLUNTÁRIA DO BEM PELA VÍTIMA. ESTELIONATO. NÃO CONFIGURAÇÃO. TIPIFICAÇÃO ADEQUADA. FURTO QUALIFICADO. MEDIANTE FRAUDE ELETRÔNICA. COMPETÊNCIA. LUGAR DA CONSUMAÇÃO. INGRESSO DOS

> VALORES NAS CONTAS DESTINATÁRIAS DAS TRANSFERÊNCIAS. LOCALIDADES DISTINTAS. PREVENÇÃO. CONFLITO CONHECIDO PARA DECLARAR COMPETENTE OJUÍZO SUSCITANTE.1. Para que se configure o delito de estelionato (art. 171 do Código Penal), é necessário que o Agente, induza ou mantenha a Vítima em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento, de maneira que está lhe entregue voluntariamente o bem ou a vantagem. Se não houve voluntariedade na entrega, o delito praticado é o de furto mediante fraude eletrônica (art. 155, §4.º-B, do mesmo Estatuto). 2. No caso concreto, não houve entrega voluntária dos valores pela Vítima, mas, sim, ocorreu a contratação de empréstimos vinculados à sua conta corrente em agência bancária na cidade de Santa Helena/MA, bem como a transferência dos valores a contas situadas no Estado de São Paulo, por meio de fraude eletrônica.3. Em se tratando de furto, a consumação do delito ocorre quando o autor do delito obtém a posse do bem. Na situação dos autos, a consumação delitiva ocorreu quando os valores ingressaram nas contas destinatárias dos valores, todas em agências localizadas no Estado de São Paulo, nas comarcas de Campinas, Itaim Paulista e São Paulocapital.4. Sendo igualmente competentes os mencionados Juízos paulistas, a competência é firmada pela prevenção, nos termos dos art. 71 e 83 do Código de Processo Penal que, no presente feito, é do Juízo campineiro, porque o único dos referidos Juízos do Estado de São Paulo que nele proferiu decisão.5. Conflito conhecido para declarar competente o JUÍZO DE DIREITO DA5.ª VARA CRIMINAL DE CAMPINAS - SP, o Suscitante. (STJ- CC 181538 / SP 2021/0243927-8)

2.3.2 Crimes contra a honra (Calúnia, Injúria e Difamação)

A honra está ligada a dignidade, perante tributos morais, valor pessoal e direito à reputação. De acordo com Paulo Lúcio Nogueira (1995, p. 116):

> A honra, considerada como um conjunto de atributos morais e intelectuais de uma pessoa, que o fazem merecedor do apreço social, é um bem tutelado pela ordem jurídica. A ofensa a esse bem é repudiada pelo Código Penal, que define três figuras ou formas de crimes contra a honra: calúnia, injúria e difamação. Caluniar alguém é atribuir-lhe falsamente a prática de delito (CP, art. 138). Difamação é a imputação de fato ofensivo à reputação da vítima (CP, art. 139). A injúria ocorre quando o agente atribui a outrem qualidade negativa, ofensiva de sua dignidade ou decoro (CP, art. 140). Essas três figuras de crime podem ser cometidas por intermédio da palavra escrita ou oral, gestos e meios simbólicos. Esses são os "meios comuns" de execução dos crimes contra a honra e, quando assim praticados regulam-se pelas disposições citadas do Código Penal.

A calúnia é o crime que ocorre quando alguém falsamente divulga ou propaga determinada informação que pode prejudicar a honra objetiva, ferindo a imagem de alguém para a sociedade. Para ocorrer o delito de calúnia a acusação deverá ser falsa e o fato criminoso, se não se tornará difamação.

A difamação é a imputação de determinado fato, verdadeiro ou não, que possa se tornar ofensivo a reputação. O que diferencia a difamação da injúria é a imputação de fato determinado. De acordo com Júlio Fabbrini Mirabete (2006, p. 134),

> A difamação é a imputação a alguém de fato ofensivo a sua reputação. Distingue-se da calúnia porque nesta o fato imputado é previsto como crime, devendo ser falsa a imputação, em regra, o que não ocorre quanto à difamação. Ambos são crimes comuns, podendo ser praticado por qualquer pessoa. Cometida através dos meios de comunicação, seja o agente profissional ou não, a difamação é crime previsto na lei de imprensa.

O crime de difamação exige dolo, como tipo subjetivo, sendo direto ou eventual, pois o agente tem a consciência e vontade de proferir fato ofensivo a outro, mesmo que não possa prever resultado.

Por fim, a injúria é a utilização de palavras ou gestos ultrajantes que serão ofensivos ao sentimento de dignidade alheio. É caracterizada pela exteriorização do desprezo e do desrespeito. De acordo com o artigo 140, §2º do Código Penal, a injúria real é caracterizada pela prática de violência, com vias de fato.

Atualmente, as penas são baseadas na aplicabilidade dos crimes que já ocorriam fora do meio virtual, diante a precariedade de legislação, juntamente com a falta de conhecimentos específicos perante os meios telemáticos. Ademais, com a facilidade de acesso a redes sociais com intensa abrangência de público, crimes como os citados acima podem se tornar ainda mais frequentes. Arthur José Concerino (2001, p.153) descreve sobre tal fato:

> Embora esteja sendo aplicada a legislação comum a crimes praticados através da rede, o fato é que em determinadas situações, o grau de ofensa ao bem da vida lesado severas, veiculadas através de normas específicas. A demais, em matéria penal, faz-se mister a descrição de uma conduta específica, pois este ramo do direito repele o uso da analogia.

2.3.3 Crime de discriminação

De maneira inicial, a lei 7.716/89 punia os crimes resultantes de preconceito de raça ou cor, conhecida como lei do racismo. Ademais, a lei nº 9.459/97 acrescentou a mesma termos como etnia, religião e procedência nacional, também como crimes de discriminação.

De acordo com o artigo 3º, IV, da Constituição Federal, a discriminação é proibida, no qual entre os objetivos fundamentais da República Federativa do Brasil se baseiam na promoção do bem de todos, sem preconceito de origem, raça ou sexo. A prática da discriminação e do preconceito por raça, etnia, cor, religião ou procedência nacional está prevista na Lei 7.716/89,

alterada pela Lei 9.459/97, de acordo com o artigo 5º, inciso XLI, que estabeleceu a prática do racismo como crime inafiançável e imprescritível, sujeito a pena de reclusão.

A pessoa que for vítima de discriminação, poderá denunciar o crime de maneira anônima às autoridades especializadas no combate aos crimes contra a honra que acontecem no meio virtual. Se a denúncia for verdadeira, o acusado que fez qualquer tipo de discriminação pelo meio telemático poderá ser condenado a reclusão de dois a cinco anos e multa.

No ano de 2012, a 1º Turma Criminal do TJDFT manteve condenação de homem que se autodenominava como Skinhead, e fazia apologia ao racismo contra judeus, negros e nordestinos em sites da internet. A denúncia foi feita pelo MPDFT que imputou ao réu prática de crime previsto no artigo 20, §2º, da Lei 7.716/89. A decisão se baseou na conduta doloso e no preconceito praticado pelo infrator.

> Ante o exposto, alicerçado no contexto fático-probatório coligido aos autos, e, diante dos argumentos já expendidos, JULGO PROCEDENTE a pretensão punitiva estatal deduzida na denúncia para CONDENAR o acusado LEONARDO LÍCIO DO COUTO, como incurso nas penas do artigo 20, § 2º, da Lei n. 7.716/89. ANTE O EXPOSTO, CONDENO O RÉU LEONARDO LÍCIO DO COUTO, DEFINITIVAMENTE, ÀS PENAS DE 2 (DOIS) ANOS DE RECLUSÃO E 10 (DEZ) DIAS-MULTA, ESTES NO VALOR UNITÁRIO EQUIVALENTE A UM SALÁRIO MÍNIMO VIGENTE AO TEMPO DO FATO DELITUOSO, DEVIDAMENTE CORRIGIDO. Considerando as condições pessoais do réu, especialmente as circunstâncias judiciais favoráveis (art. 33, § 3º, do CP), o regime de cumprimento de pena será, inicialmente, o aberto, conforme dispõe o artigo 33, caput, § 2º, alínea "c", do Código Penal. Tendo em vista o preenchimento dos requisitos do art. 44, do CP, substituo a pena privativa de liberdade por uma pena restritiva de direito e uma pena de multa. A primeira, a ser fixada pelo Juízo das Execuções. A segunda, ora fixada em dez salários mínimos correntes, haja vista a capacidade econômica do réu. Em 21/08/2014. Recurso apelação criminal. Desprovido. Unânime. Em 05/03/2015. Embargos de declaração na apelação criminal. Desprovido. Unânime. Em 26/03/2015. Indeferido o processamento dos recursos especial e extraordinário. Em 14/07/2015. Agravo conhecido para negar provimento ao recurso especial. Em 24/02/2017. Agravo Regimental negado provimento. Em 24/05/2018. Embargos de declaração rejeitados. Em 26/06/2018. Embargos de divergência não conhecidos, por serem manifestamente incabíveis, além de denotar caráter protelatório e inaceitável ato atentatório à dignidade da Justiça. Determinada a certificação do trânsito em julgado do acórdão embargado, independentemente de apresentação de nova petição pelo embargante, com imediata remessa dos autos para o STF para apreciação do agravo em recurso extraordinário. Em 09/10/2018. Trânsito em julgado no STJ em 16/10/2018. Agravo em Recurso Extraordinário negado seguimento. Em 01/02/2019. Agravo Regimental negado Provimento. Em 22 a 28 de março de 2019. Embargos de Declaração rejeitados, determinando-se o trânsito em julgado e a baixa imediata dos autos à origem. Em 17 a 23 de maio de 2019. (Processo n. 2012.01.1.098316-9)

2.3.4 Incitação e apologia ao crime

As redes sociais se tornarem uma base para pessoas que fazem apologia e incitação ao crime, com publicações que giram em torno de apoio a atos de vandalismo e a crimes puníveis no ordenamento jurídico brasileiro. Ambos crimes são os que ganham mais espaço no Brasil. Segundo a entidade SaferNet, que reúne cientistas da computação e pesquisadores e bacharéis em direito que visam a defesa e a promoção dos direitos humanos na internet, em artigo publicado no ano de 2018, desde o ano de 2006 já foram encontradas 2.768 páginas com apoio e incitação ao crime contra a vida, sendo que no ano de 2015 esses mesmo crimes ficaram em segundo lugar entre os três mais cometidos na internet, ficando atrás apenas do crime de racismo.

A incitação é o estímulo a prática de determinado crime de forma pública, não tendo um público alvo específico que se pretenda atingir. A apologia é a defesa de um fato criminoso ou do autor de um crime, também de forma pública.

A denúncia de divulgação de vídeos, comentários ou compartilhamentos que apoiam a violência ou o crime se enquadram nos artigos 286 e 287 do Código Penal Brasileiro, com pena de detenção.

> Incitação ao crime
> Art. 286 - Incitar, publicamente, a prática de crime:
> Pena - detenção, de três a seis meses, ou multa.
> Apologia de crime ou criminoso
> Art. 287 - Fazer, publicamente, apologia de fato criminoso ou de autor de crime:
> Pena - detenção, de três a seis meses, ou multa

2.3.5 Pirataria

A pirataria no meio telemático se refere ao uso e/ou distribuição não autorizada de materiais que são protegidos por direitos autorais na internet. As formas mais comuns de distribuição da pirataria na rede de computadores são sites, plataformas e aplicativos sem relação com emissoras e produtoras que disponibilizam séries, novelas e outros programas televisivos, além de endereços online e compartilhamento de arquivos torrent.

Ademais, os produtores acabam perdendo investimentos devido a distribuição ilegal de conteúdo que não gera renda para os mesmos, violando de maneira direitos os direitos autorais, conforme o artigo 184 do Código Penal brasileiro.

> Art. 184. Violar direitos de autor e os que lhe são conexos:
> Pena – detenção, de 3 (três) meses a 1 (um) ano, ou multa.
> § 1º Se a violação consistir em reprodução total ou parcial, com intuito de lucro direto ou indireto, por qualquer meio ou processo, de obra intelectual,

> interpretação, execução ou fonograma, sem autorização expressa do autor, do artista intérprete ou executante, do produtor, conforme o caso, ou de quem os represente:
> Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
> § 2º Na mesma pena do § 1º incorre quem, com o intuito de lucro direto ou indireto, distribui, vende, expõe à venda, aluga, introduz no País, adquire, oculta, tem em depósito, original ou cópia de obra intelectual ou fonograma reproduzido com violação do direito de autor, do direito de artista intérprete ou executante ou do direito do produtor de fonograma, ou, ainda, aluga original ou cópia de obra intelectual ou fonograma, sem a expressa autorização dos titulares dos direitos ou de quem os represente.
> § 3º Se a violação consistir no oferecimento ao público, mediante cabo, fibra ótica, satélite, ondas ou qualquer outro sistema que permita ao usuário realizar a seleção da obra ou produção para recebê-la em um tempo e lugar previamente determinados por quem formula a demanda, com intuito de lucro, direto ou indireto, sem autorização expressa, conforme o caso, do autor, do artista intérprete ou executante, do produtor de fonograma, ou de quem os represente:
> Pena – reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
> § 4º O disposto nos §§ 1º, 2º e 3º não se aplica quando se tratar de exceção ou limitação ao direito de autor ou os que lhe são conexos, em conformidade com o previsto na Lei nº 9.610, de 19 de fevereiro de 1998, nem a cópia de obra intelectual ou fonograma, em um só exemplar, para uso privado do copista, sem intuito de lucro direto ou indireto.

Outrossim, por ser um crime que ocorre nos meios telemáticos, que acaba dificultando a identificação de infratores, ocorreu entendimento de jurisprudência diante a não necessidade de comprovação do completa do crime. De acordo com entendimento da Terceira Seção do Superior Tribunal de Justiça no julgamento de dois recursos cadastrados sob o número 926, para se tornar crime de violação autoral não será necessário fazer perícia em todos os bens apreendidos nem identificar os titulares dos direitos violados, sendo necessária apenas a comprovação de materialidade do delito, como descrito no parágrafo 2º do artigo 184 do CP.

> RECURSO ESPECIAL. PROCESSAMENTO SOB O RITO DO ART. 543-C DO CÓDIGO DE PROCESSO CIVIL. RECURSO REPRESENTATIVO DA CONTROVÉRSIA. VIOLAÇÃO DE DIREITO AUTORAL. PERÍCIA SOBRE TODOS OS BENS APREENDIDOS. DESNECESSIDADE. ANÁLISE DOS ASPECTOS EXTERNOS DO MATERIAL APREENDIDO. SUFICIÊNCIA. IDENTIFICAÇÃO DOS TITULARES DOS DIREITOS AUTORAIS VIOLADOS. PRESCINDIBILIDADE. RECURSO PROVIDO.
> 1. Recurso Especial processado sob o regime previsto no art. 543-C, § 2º, do CPC, c/c o art. 3º do CPP, e na Resolução n. 8/2008 do STJ. TESE: É suficiente, para a comprovação da materialidade do delito previsto no art. 184, § 2º, do Código Penal, a perícia realizada, por amostragem, sobre os aspectos externos do material apreendido, sendo desnecessária a identificação dos titulares dos direitos autorais violados ou de quem os represente. 2. Não se exige, para a configuração do delito previsto no art. 184, § 2º, do Código Penal, que todos os bens sejam periciados, mesmo porque, para a caracterização do mencionado crime, basta a apreensão de um único objeto.

> 3. A constatação pericial sobre os aspectos externos dos objetos apreendidos já é suficiente para revelar que o produto é falso. 4. A violação de direito autoral extrapola a individualidade do titular do direito, pois reduz a oferta de empregos formais, causa prejuízo aos consumidores e aos proprietários legítimos, fortalece o poder paralelo e a prática de atividades criminosas, de modo que não é necessária, para a caracterização do delito em questão, a identificação do detentor do direito autoral violado, bastando que seja comprovada a falsificação do material apreendido. 5. Recurso especial representativo da controvérsia provido para reconhecer a apontada violação legal e, consequentemente, cassar o acórdão recorrido, reconhecer a materialidade do crime previsto no art. 184, § 2º, do Código Penal e determinar que o Juiz de primeiro grau prossiga no julgamento do feito (Processo n. 0024.12.029829-4)

2.4 Meios telemáticos como elementar do tipo

Na mesma proporção do crescimento de benefícios que a internet trouxe para a sociedade, condutas ilícitas começaram a ser praticadas. Tais condutas podem ser entendidas como crimes virtuais, crimes cibernéticos, digitais, telemáticos, crimes de rede, entre outros.

Ivette Senise Ferrreira (2005, p. 261) descreve a seguinte classificação de crimes virtuais:

> Atos dirigidos contra um sistema de informática, tendo como subespécies atos contra o computador e atos contra os dados ou programas de computador. Atos cometidos por intermédio de um sistema de informática e dentro deles incluídos infrações contra o patrimônio; as infrações contra a liberdade individual e as infrações contra a propriedade imaterial.

Ademais, os crimes cibernéticos possuem algumas diferenciações. Os delitos informáticos próprios, ou puros, são aqueles em que o sujeito ativo utiliza o sistema informático do sujeito passivo, ou seja, o computador é utilizado como sistema tecnológico para ser objeto e meio para o crime. Nessa conceituação sobre o crime está a invasão de dados armazenados em computadores que possuam o intuito de modificar, alterar ou inserir dados ilícitos, podendo atingir diretamente software ou hardware do computador e seus periféricos.

Os crimes virtuais impróprios são realizados com a utilização do computador e da rede, são aqueles violam bens já protegidos pela legislação brasileira, e podem ser praticados de qualquer forma, utilizando o computador apenas como meio/instrumento para a conduta ilícita. Tais crimes já estão disposto no Código Penal nos artigos 138 a 140, como os crimes contra a honra, envolvendo calúnia, difamação e injúria. O artigo 147 também do CP abrange o crime contra a ameaça, que consiste em escrever, mostrar, ou publicar algo que possa atingir outra pessoa com a intenção de algo. Já o artigo 171 do mesmo código abrange o crime contra o

patrimônio, como o estelionato, que pode ocorrer por meio da enganação do sujeito para conseguir vantagem financeira.

O 8º Congresso sobre Prevenção de Delito e Justiça Penal, que ocorreu em 1990, em Havana, Cuba, apresentou uma publicação da ONU sobre a relação de crimes informáticos, que reconheciam alguns delitos. As fraudes cometidas mediante manipulação de computadores por meio de dados de entrada ou saída, conhecidas também como manipulação de programas, forjamento de objetivos ou funcionamentos do sistema informático, além da manipulação informática, que utiliza de repetições automáticas dos processos do computador para golpes financeiros. As falsificações informáticas, que podem alterar dados de documentos armazenados em formato computadorizado, como a falsificação de documentos de uso comercial. E por fim, os danos ou modificações de programas computadorizados, conhecidos também como a sabotagem informática, que é o ato de copiar, suprimir ou modificar sem autorização funções ou dados informáticos.

Em consonância com os danos ou modificações de programas ou dados computadorizados é possível que se apresente algumas técnicas como vírus, que são séries de chaves programadas para aderir a programas legítimos e propagar-se por outros meios informáticos. Gusanos, que infiltram em programas legítimos com intuito de modifica-los ou destruí-los. Bomba lógica ou cronológica, que necessitam de conhecimentos especializados para a programação de destruição ou modificação de dados em um determinado momento futuro. O acesso não autorizado a sistemas de serviços, como a sabotagem e a espionagem informática. Os piratas informáticos que aproveitam de falhas nos sistemas de segurança para poder acessar programas ou órgãos de informações e, por fim, a reprodução não autorizada de programas informáticos de proteção legal, podendo causar perda econômica substancial a proprietários intelectuais legítimos.

No 10º Congresso sobre Prevenção de Delito e Tratamento de Delinquente, em Viena, no ano 2000, a ONU publicou novamente tipos de delitos informáticos. A espionagem industrial consiste no avanço realizado por pirataria para empresas ou próprio proveito, copiando segredos comerciais que abordam informações sobre técnicas ou produtos diante estratégias de comercialização. A sabotagem de sistemas que utilizam de bombardeio eletrônico para envio de mensagens repetidas a um site, impedindo acesso legítimo aos mesmos. A sabotagem e o vandalismo de dados que ocorre quando intrusos acessam sites eletrônicos, ou bases de dados, apagando-os ou alterando-os de forma a corromper os dados. A pesca ou averiguação de senhas secretas são quando ocorre o roubo de senhas pessoais por meio de enganação, com infratores se passando por agentes de lei ou empregados de provedores de serviço, os mesmos utilizam de

programas que identificam senhas de usuários, utilizando-as sem autorização para acesso ao sistema de computadores, delitos financeiros, vandalismo e até mesmo atos terroristas.

Foram apresentados também outros delitos informáticos como a estratagemas, que consiste na ocultação de computadores que se parecem com outros, para poder lograr e acessar sistemas restritos para cometer delitos. A pornografia infantil ocorre com a distribuição de fotos, vídeos ou quaisquer outros modelos que apresentam crianças e adolescentes como objetos sexuais, esse crime se agrava quando se tem novas tecnologias como a criptografia, que torna a descoberta de infratores mais complicada. Os jogos de azar no meio eletrônico se tornaram um comércio com intuito de facilitar créditos e transferências de fundos pela rede. A fraude oferta para consumidores vendas, premiações, ou promoções que podem cotizar ações, bônus e valores ou até mesmo a venda de equipamentos ilícitos por meio de e-commerce. Por fim, foi apresentado a lavagem de dinheiro, que pelo e-commerce tornou-se possível a transferência de mercadorias e dinheiro para o crime, mediante ocultação de transações.

CAPÍTULO 3 – CRIMES ELETRÔNICOS E A LEI BRASILEIRA

3.1 Pornografia Infantil e Pedofilia com uso de meios telemáticos (artigos 241-A e 241-E do Estatuto da Criança e do Adolescente)

O crescente uso das redes por todas as faixas etárias para diversos fins, juntamente com a facilidade do anonimato, fazem da internet um meio perigoso para uso sem controle de crianças e adolescentes. O mercado de prostituição e pornografia infantil nos meios telemáticos tem sido disseminado diante o fácil acesso de pedófilos a menores por meio de sites de relacionamentos, com compartilhamentos de fotos, vídeos e informações dos mesmos.

Para a Organização Mundial da Saúde a pedofilia é considerada uma doença, visto como um transtorno de sexualidade, que consiste na preferência sexual por meninos ou meninas, envolvendo desejos e fantasias com crianças. Pedofilia, portanto, é um termo médico, cujo diagnóstico depende de uma reiteração de fantasias durante um período mínimo de seis meses, pois é vista como um estado e não apenas como uma ação, dado como um padrão frequente de desejo e impulso no qual o indivíduo sente atração sexual por crianças. Entretanto, não se pode considerar o abuso de crianças apenas como "doença" pois os infratores acabam trazendo diversos perigos para a sociedade.

Já no meio jurídico, o objeto é a tutela penal diante a integridade moral e física de crianças e adolescentes. O sujeito ativo pode ser qualquer pessoa, e o tipo subjetivo é o dolo, ou seja, é a vontade livre e consciente do infrator em realizar determinado ato, como vender ou expor.

Os abusos sexuais que são cometidos no Brasil podem configurar diversos crimes, como a pornografia infantil e a pedofilia com uso de meios telemáticos. O artigo 241 da Lei 8.069/90 (ECA) tipifica como crime o fato de fotografar ou publicar cena de sexo explícito ou pornográfica envolvendo crianças e adolescentes, podendo ter pena de 1 (um) a 4 (quatro) anos de reclusão.

A pornografia Infantil e pedofilia são expressas nos artigos 241-A e 241-E do Estatuto da Criança e do Adolescente, que sinalizam também sobre os crimes praticados em meio telemático.

> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Incluído pela Lei nº 11.829, de 2008)

> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa. (Incluído pela Lei nº 11.829, de 2008)
> § 1º Nas mesmas penas incorre quem:
> I – Assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;
> II – Assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.
> § 2º As condutas tipificadas nos incisos I e II do § 1o deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo.
> Art. 241-E. Para efeito dos crimes previstos nesta Lei, a expressão "cena de sexo explícito ou pornográfica" compreende qualquer situação que envolva criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou exibição dos órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais. (Incluído pela Lei nº 11.829, de 2008)

A inclusão das condutas que ocorrem na rede mundial de computadores, demonstra a facilidade de cometimento do crime utilizando-se dos meios eletrônicos. Entretanto, de acordo com os artigos acima a pedofilia não é tipificada como um crime, mas como conduta praticada por pedófilo, que cometem crimes previstos no Código Penal e no Estatuto da Criança e do Adolescente. O verbo "publicar" no artigo 241-A (ECA) adequa-se ao meio telemático, trazendo a ideia de uso da internet como um meio de troca de matérias e exposição para crianças e adolescentes. Em todo o artigo 241 do Estatuto da Criança e do Adolescente se encontram verbos como "apresentar", "produzir", "fornecer" e "divulgar", tanto fotografias quanto qualquer outro meio que dissemine imagens de abuso contra menores.

A presença dos verbos citados anteriormente abrangeu as condutas praticadas por qualquer meio de comunicação, sendo rede mundial de computadores ou qualquer aparelho que possa ter acesso a internet, trazendo a ideia que os meios telemáticos não possuem acesso restrito ao público, e o seu uso de forma indevida pode acarretar problemas.

Entretanto, em muitos casos não se tem exposição gráfica do material na Internet, e apenas são disponibilizados pedaços de arquivos que sozinhos não representam graficamente nada. Somente após download dos "pedaços" e sua unificação posteriormente surge a representação multimídia da infração.

A sociedade pós-industrial com intenso acesso a rede de computadores faz da juventude um alvo fácil nas redes, por terem conhecimento de sites de relacionamentos e subjacentes e socializarem informações a todo e qualquer usuário do meio telemático. Com a facilidade de acesso, principalmente, por smartphones, cada vez mais novas as crianças acessam e dominam a tecnologia, agregando-se em um meio de informação difuso, abundante e perigoso se usado sem os devidos cuidados.

Diante o exposto anteriormente, programas como CyberPatrol, CyberSitter, BESS, WebSense, Smart Filter, X-Stop, I-Gear, NetNanny e muitos outros visam regular os conteúdos acessíveis por crianças e adolescentes, como fotos, vídeos e sites de conteúdos inapropriados, e funcionam como uma maneira de bloqueio para impedir o acesso a sites e conteúdos inapropriados, filtrando de acordo com a determinação de um usuário por meio do controle de administrador. Tais programas visam afastar o contato de menores com materiais que poderiam leva-lo para rumos desaconselháveis pela ciência. Entretanto, a imaturidade do adolescente frente a novas descobertas, principalmente nos meios telemáticos fazem com que a rede mundial de computadores sirva como um catalisador, ou seja, faz com que informações, atos, e pessoas com más intenções tenham acesso a essas crianças de maneira mais rápida.

Outrossim, a pornografia infantil e a pedofilia com uso de meios telemáticos além do envolvimento de crianças e adolescentes pela facilidade de acesso e propagação de imagens e vídeos, possui também desafios diante a identificação dos criminosos, pois a internet é um meio que proporciona um anonimato com maior facilidade com uma difícil localização do infrator.

Os Tribunais diante um caso concreto, fazem analogia de princípios do direito para a resolução de ocorrência que envolvem a pedofilia no meio virtual. Como exemplo, o informativo nº 0507 publicado de 18 a 31 de outubro de 2012 no site do Superior Tribunal de Justiça descreve a competência diante o processo e julgamento da pornografia infantil em redes de internet.

> Compete à Justiça Federal processar e julgar as ações penais que envolvam suposta divulgação de imagens com pornografia infantil em redes sociais na *internet*. A jurisprudência do STJ entende que só a circunstância de o crime ter sido cometido pela rede mundial de computadores não é suficiente para atrair a competência da Justiça Federal. Contudo, se constatada a internacionalidade do fato praticado pela internet, é da competência da Justiça Federal o julgamento de infrações previstas em tratados ou convenções internacionais (crimes de guarda de moeda falsa, de tráfico internacional de entorpecentes, contra as populações indígenas, de tráfico de mulheres, de envio ilegal e tráfico de menores, de tortura, de pornografia infantil e pedofilia e corrupção ativa e tráfico de influência nas transações comerciais internacionais). O Brasil comprometeu-se, perante a comunidade internacional, a combater os delitos relacionados à exploração de crianças e adolescentes em espetáculos ou materiais pornográficos, ao incorporar, no direito pátrio, a Convenção sobre Direitos da Criança adotada pela Assembleia Geral das Nações Unidas, por meio do Decreto Legislativo n. 28/1990 e do Dec. n. 99.710/1990. A divulgação de imagens pornográficas com crianças e adolescentes por meio de redes sociais na internet não se restringe a uma comunicação eletrônica entre pessoas residentes no Brasil, uma vez que qualquer pessoa, em qualquer lugar do mundo, poderá acessar a página publicada com tais conteúdos pedófilo-pornográficos, desde que conectada à internet e pertencente ao sítio de relacionamento. Nesse contexto, resta

> atendido o requisito da transnacionalidade exigido para atrair a competência da Justiça Federal. Precedentes citados: CC 112.616-PR, DJe 1º/8/2011; CC 106.153-PR, DJ 2/12/2009, e CC 57.411-RJ, DJ 30/6/2008. CC 120.999-CE, Rel. Min. Alderita Ramos de Oliveira (Desembargadora convocada do TJ-PE), julgado em 24/10/2012.

3.2 Invasão de dispositivo informático (artigos 154-A e 154-B do Código Penal)

Com o desenvolvimento dos meios informacionais e o crescente acesso aos mesmos, as trocas de informações na rede acabaram se intensificando. Contudo, os crimes informáticos também começam a aparecer, como a invasão de dispositivo informático.

A jurisprudência passa a equiparar a invasão de dispositivo informático ao crime de interceptação de comunicação, previsto no artigo 10º da Lei 9.296/96, que descreve como crime "realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei". O Tribunal de Justiça de Santa Catarina apresentou esse fato em um de seus julgados: "A conduta de quem 'invade' provedor de Internet, apropriando-se dos logins e senhas de seus usuários e, assim, 'invadindo' seus computadores, os quais tinham livre e desimpedido acesso, podendo inclusive apagar arquivos do sistema, como, de fato, o fez" (Apelação Criminal n. 2007.006842-9, Rel. Des. Irineu João da Silva, julgado em 22/5/2007).

O conceito de interceptação pressupõe que sejam captados dados e informações de comunicações que estejam em curso, fazendo com que a aplicação da invasão do dispositivo informacional inserida na mesma lei se torne frágil, pois a invasão do mesmo pode ocorrer de diversas formas, mesmo sem ocorrer interceptação.

Nesse contexto se insere a Lei n. 12.737/12, conhecida como Lei Carolina Dieckmann, em referência a atriz que teve sua privacidade invadida, com acesso indevido a seu computador e divulgação de suas fotos íntimas na internet. Com esse fato, foram inseridos os artigos 154-A e 154-B no Código Penal Brasileiro. A inserção desse tipo penal descreve a invasão de dispositivo informático alheio, conectado ou não à rede de computadores por meio de violação indevida de mecanismo de segurança, com fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo, ou até mesmo instalando programas que possam servir para obtenção de dados de maneira ilícita.

O projeto que deu origem a lei 12.731/12 foi baseada na oportunidade de garantia de repressão a condutas socialmente indesejáveis, sem uma criminalização excessiva. A lei que se encontra em vigor desde abril de 2013 não definiu de maneira específica o que seria o "dispositivo informático" para efeitos penais, para fim de aplicação da mesma pode se explicar

dispositivo informático como algo capaz de armazenar dados, informações e documentos em meio digital, por meio de computadores, smartphones, ou semelhantes.

O artigo 154-A do Código Penal Brasileiro descreve:

> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: (Redação dada pela Lei nº 14.155, de 2021)
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (Redação dada pela Lei nº 14.155, de 2021)

Nos parágrafos do mesmo artigo é apresentado também que a mesma pena poderá incorrer com quem produz, oferece, distribui, vende, ou difunde dispositivo que possa demonstrara ou permitir prática de conduta ilícita. Ademais, demonstra também que se a invasão resultar em acesso a conversas eletrônicas privadas ou sigilosas, definidas em lei, a pena será de reclusão de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não demonstrar crime mais grave, entretanto, a pena será aumentada de houver divulgação, comercialização ou transmissão de dados obtidos de maneira ilícita, para um terceiro. O mesmo crime também não poderá ser praticado contra representantes políticos, podendo ser aumentado de um terço à metade da pena.

Diante o exposto, o crime previsto no artigo 154-A do CP é considerado crime de menor potencial ofensivo, por ter pena máxima inferior a dois anos. Ademais, poderá ser praticado por qualquer pessoa, não seno necessário que se prove que o autor do delito possa ser um hacker, que tenha habilidades especiais para acesso a dispositivos informáticos. Entretanto, mesmo que o agente não obter, adulterar ou destruir dados por meio da invasão, ainda se tem a consumação do delito, mesmo alcançando ou não o resultado previsto no tipo penal.

Se tratando de crime doloso, será punível quando o agente demonstrando interesse em obter resultado ou assumir risco de produzi-lo, sendo necessário a presença de dolo específico, no qual a intenção do agente seja obter, adulterar, instalar vulnerabilidades, ou destruir dados e informações. Entretanto, nem sempre a invasão sem permissão caracterizará crime, para que se tenha a consumação do delito é necessário que ocorra a invasão seguida da violação indevida de mecanismos de segurança sem autorização. No artigo 154-A a ação penal é pública, ou seja, condicionada a representação, só havendo denúncia se a vítima manifestar sua vontade. E a competência de processar e julgar de acordo com o artigo 61 da Lei 9.099/95, será dos Juizados Especiais Criminais.

No artigo 154-B do Código Penal é descrito:

> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime e 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. (Incluído pela Lei nº 12.737, de 2012)

Quando o crime for cometido contra a Administração Pública Direta ou Indireta, ou contra empresas concessionárias de serviços públicos, a ação penal passa a ser pública incondicionada, ou seja, a promotoria poderá oferecer denúncias sem ter provas concretas diante o cometimento do delito ou até mesmo de sua autoria.

Luiz Regis Prado (2014, p. 596) descreve:

> A ação penal nos delitos definidos pelo artigo 154-A é pública condicionada, salvo se o crime é cometido contra administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos, hipótese em que a ação é pública incondicionada.

Ademais, com o advento do acesso à internet e a evolução da mesma, ocorreram melhorias e, ao mesmo tempo, o aumento da vulnerabilidade perante crimes que podem acontecer no meio cibernético. Nos dias atuais é possível distinguir o crime cibernético após o advento da Lei 12.737/12, trazendo a possibilidade de punição específica de acordo com os artigos 154-A e 154-B do Código Penal. Entretanto, delitos que ocorrem no meio cibernético ainda são difíceis de serem processados e julgados, diante da dificuldade para encontrar a autoria do delito, sendo a internet um meio difícil de deixar rastros, no qual é difícil identificar onde surgiu o ato praticado e a motivação para a consumação do mesmo.

3.3 Análise do direito comparado face a convenção europeia de cyber crimes

A convenção de Budapeste que ocorreu no ano de 2001 promoveu a criação de normas específicas para o ordenamento jurídico internacional. O documento foi desenvolvido pelo Conselho Europeu e estabeleceu normas, condutas, métodos e diretrizes para intervenções, voltadas ao combate aos cibercrimes. Ademais, o texto criou instrumentos legais específicos para a interpretação, investigação e apreciação de delitos que ocorrem no meio eletrônico. O tratado estabelece medidas de maneira repressiva, preventiva e punitiva de acordo com a coleta de provas vindas de provedores.

Em seu artigo 28, o tratado descreve um plano de assistência mútua *transborder*, que busca combater os crimes ocorridos no ciberespaço, mesmo que seja em territórios geograficamente distintos. Ou seja, a interpretação do tratado envolvia a cooperação entre territórios em prol da justiça.

A Convenção possui um escopo principal que busca harmonizar o direito penal interno (de cada país) e harmoniza-lo de acordo com as previsões previstas em relação ao cibercrime, dispor perante o direito processual penal interno de poderes necessários para investigação e repressão de delitos cometidos em sistemas de computador e, por fim, a criação de um regime de cooperação internacional rápido e eficaz.

Gonçalo Souza (2017, p.108-114), em artigo escrito para a 1º Conferência Internacional de Lisboa sobre Segurança da Informação e Direito Constitucional do Ciberespaço, descreve que é necessário um entendimento jurídico que possa regulamentar o ambiente virtual, sendo indispensável para a harmonia e o desenvolvimento social, abrangendo questões que norteiam a segurança nacional e os cibercrimes.

> É inadiável a publicação de uma Lex informática que evolua de um conjunto de regras sobre fluxos de informação imposta pela tecnologia e redes de comunicações. É ainda necessária uma análise legal multidisciplinar e funcional, assim como mais regulação que permita delinear os limites da moldura legal atual, reforçando a segurança Nacional, enfrentando o cibercrime e minimizando a utilização da Internet pelos terroristas.

Entretanto, na época da Convenção o Ministério das Relações Exteriores se opôs à adesão do Brasil à Convenção, alegando que não houve composição do país da redação do termo, com normas que não seriam compatíveis com o ordenamento jurídico brasileiro vigente na época. Desde sua adoção 54 estados adotaram a Convenção sobre cibercrime, atualmente, 28 já retificou, incluindo países que não integram a União Europeia como Canadá, Japão, México, Filipinas, Estados Unidos, entre outros.

Ademais, a mesma prevê também recomendações diante o direito interno dos países signatários, estabelecendo condutas delituosas diante os atos de acesso ilegítimo de maneira intencional, interceptação ilegítima de dados informáticos, interferência em dados, interferência em sistemas e uso abusivo de dispositivos, sendo necessário novas tipificações penais.

Em relação a interceptação ilegítima de dados informáticos, o artigo 5º, inciso XII, da Constituição Federal Brasileira descreve que “é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por

ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal".

Diante disso, a própria Carta Magna prevê tutela, tendo punição descrita também na Lei 9.296/96, relacionada a interceptação de ligações telefônicas, também regulamenta o disposto no artigo 5º, XII.

Outrossim, a Convenção do Conselho da Europa sobre Cibercrime, em seu Título 2 descreve sobre as infrações relacionadas a computadores, como a falsidade e a burla informática. Essas duas infrações já estão previstas na regulamentação penal brasileira, na Lei 9.983/2000, que inseriu os artigos 313-A e 313-B, que preveem punição diante a inserção de dados falsos em sistema de informação e a modificação ou alteração não autorizada dos sistemas de informação. Ademais, o Código Eleitoral em seu artigo, descrevem sobre as infrações diante o acesso indevido ao sistema de votação eletrônico ou o dano nas urnas eletrônicas.

No artigo 9º, a Convenção de Budapeste apresenta a conduta diante as infrações relacionadas a pornografia infantil na internet, que possui punição no artigo 241 do Estatuto da Criança e do Adolescente, aprimorando o combate à produção, venda ou distribuição de pornografia infantil, criminalizando a aquisição e posse de material e condutas relacionadas à pedofilia na internet. Ademais, essa medida legislativa não decorreu da adesão à Convenção, e sim da pressão exercida pela sociedade e debates parlamentares com o advento da CPI da pedofilia.

Na mesma Convenção, foi debatido sobre o direito autoral. No Brasil a lei nº 9.609/98 dispõe sobre a propriedade intelectual de programas de computadores e comercialização. A Lei nº 10.695/2003 alterou as disposições presentes no Código Penal Brasileiro de acordo com o mesmo assunto. As duas legislações abrangem a Convenção de Budapeste com base no direito material.

Sobre as medidas necessárias de responsabilização e punição de delitos, foi exposto no título 5, art. 11, da Convenção de Budapeste. Em relação ao mesmo, o art. 12º refere à disponibilidade penal da pessoa jurídica em face de crimes praticados, de forma individual ou de forma omissiva, demonstrando negligência perante a supervisão e o controle de atividades exercidas por empregados. Já o artigo 13º, o instrumento jurídico internacional, descreve a necessidade que os Estados signatários tomem medidas em relação a asseguração de infrações penais, possuindo sanções eficazes, proporcionais e dissuasivas, incluindo pena privativa de liberdade. No ordenamento Brasileiro, o art. 14 e o art.29 do Código Penal Brasileiro apresenta semelhança entre as disposições.

De acordo com o artigo 35 da Convenção, os estados membros devem disponibilizar uma rede durante seite dias da semana, vinte e quatro horas por dia como ponto de contato para que todos os países membros possam prestar auxílio nas investigações e procedimentos relacionados a crimes cibernéticos. Para o Brasil, isso se tornaria inviável diante a quantidade de processos e armazenamentos que deveriam ser feitos. Outros pontos como o armazenamento de informações por um provedor, na época da Convenção não seria possível para o país. Entretanto, o Marco Civil da Internet já abrange esse ponto, prevendo a proibição da guarda de registros por parte de provedores de conexão e liberando seis meses de guarda no caso de provedores de aplicação para fins econômicos.

Outrossim, será necessário a adesão do Brasil à Convenção de Budapeste, buscando uma uniformização legislativa no combate a crimes cibernéticos transnacionais , abrangendo um modelo homogêneo de aplicação de sanções em todos os países membros, garantindo uma maior variedade de instrumentos aplicáveis diante os delitos informáticos e uma maior gama de cooperação internacional, somando pontos positivos juntamente com a Lei Carolina Dieckmann e com o Marco Civil da Internet.

Em reunião que ocorreu no dia 23 de setembro de 2021 com procuradores-gerais do Mercosul, Augusto Aras defendeu a criação de unidades especializadas em crimes cibernéticos e relatou a importância da adesão do Brasil a convenção de Budapeste. “Para nós, do Ministério Público Federal, essa adesão configura prioridade e avanço crucial para a elucidação de crimes que dependem de prova digital, sendo essencial que os Ministérios Públicos possam ser autoridades centrais da cooperação internacional no âmbito desta Convenção”

Por fim, a Convenção buscou maneiras rápidas e eficazes diante a ameaças presentes no meio cibernético, baseando-se em uma cooperação internacional. Na época o Brasil não aderiu a mesma por questões diplomáticas em relação aos termos que não foram discutidos com representantes do país. Os aparatos apresentados talvez sejam o meio mais abrangente em relação ao mundo cibernético e os crimes feitos no mesmo, oferecendo conceitos e definições básicas, e melhorias diante investigações e processos de crimes virtuais, aumentando também a cooperação internacional e o combate aos cibercrimes. Portanto, seria necessário a adesão do Brasil a Convenção, abrangendo a visão em relação aos crimes cibernéticos, aumentando também a visibilidade diante outros países.

3.4 Análise das normas brasileiras tipificadoras de cibercrimes diante dos marcos normativos de proteção ao usuário da internet

A era digital que abrange a sociedade contemporânea, faz com que as pessoas em boa parte de suas vidas sejam gerenciadas por sistemas de informatização. Esses sistemas armazenam informações das mesmas, gerando dados, endereços, listas de contatos e e-mails. Ademais, por mais que pareça que o acesso a internet de maneira fácil seja algo benigno, o seu uso sem determinados cuidados pode acarretar diversos problemas, como roubo de informações pessoais, manipulação virtual, espionagem, etc.

Diante o exposto, é necessário que haja discussão acerca da proteção efetiva à privacidade e dos limites que devem ocorrer diante a coleta dos dados pessoas por sistemas, e como determinadas informações serão tratadas e repassadas. A análise diante a evolução da proteção ao direito fundamental à privacidade garantido no Brasil deve ser adequada de acordo com as novas tecnologias de informação e comunicação e como as mesmas se relacionam diante a proteção de dados pessoas na internet e em sistemas computacionais.

De acordo com Leonardi (2011, p. 402), a privacidade é dada como a capacidade do indivíduo de exercer controle sobre a circulação de informações a seu respeito, o que geralmente não é possível diante todo o uso de empresas e pessoas como um todo que a internet pode atingir.

> [...] o "conjunto de informação acerca do indivíduo que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições, sem a isso pode ser legalmente sujeito". A privacidade é, assim, "o poder de revelar-se seletivamente ao mundo" e não significa apenas o direito de ser deixado em paz, mas também "o direito de determinar quais atributos de si serão usados por outros".

No ano de 1948, durante o período da 2º Guerra Mundial, A Declaração Universal dos Direitos Humanos apresentou em seu artigo 12 entendimento diante a privacidade. "Ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques a sua honra e reputação. Toda pessoa tem direito à proteção da lei contra tais interferências ou ataques". É possível, portanto, que se observe o sentido amplo na maneira que a ONU encorajou diversos países para que os mesmos protegessem a vida privada de seus cidadãos.

No Brasil, no ano de 1967 (artigo 150, §9º), a Constituição Federal Brasileira ampliou o entendimento diante a proteção à privacidade, abrangendo não apenas a inviolabilidade de correspondências, mas também garantir o sigilo diante as comunicações do cidadão, barrando

interferências alheias. A Constituição de 1988 no seu artigo 5º, incisos X e XII, efetivou a importância do direito à privacidade e a intimidade, colocando os mesmos como direitos e garantias fundamentais dos cidadãos.

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: [...]
> 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; [...]
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; [...]

Após a chegada da internet no Brasil no ano de 1988, condutas nocivas passaram a acontecer com usuários do ambiente virtual, condutas estas não abordadas pela legislação. Projetos de Lei sobre a criminalização e a tutela da privacidade começaram a surgir como o PL 84/1999 que versava sobre criminalização de hackers e a utilização indevida de senhas, e o PL 151/2000 que resguardava diante o acesso à internet e o sigilo de dados de usuário brasileiros em *datacenters* instalados no Brasil. Ademais, com o crescente desenvolvimento das redes e do crescente acesso da população a mesma, será analisado nos próximos subtópicos leis que possuem enfoque à proteção da privacidade e dos dados pessoais.

3.4.1 Marco Civil da Internet (Lei nº 12.965/2014)

A resolução de conflitos advindos da internet envolve questões sensíveis que acabam abrangendo os provedores de acesso, os provedores de conteúdo e os usuários da rede. O Marco Regulatório Civil da Internet é o mais significativo no âmbito do direito civil, tratando de temas como a responsabilidade pelo tráfego de dados, a guarda de registros de usuários e a não responsabilidade diante possíveis danos que podem ser gerados por terceiros. Outrossim, a lei nº 12.965/2014 estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil perante provedores de acesso, aplicação e usuários, definindo os papéis e responsabilidades necessárias de cada um destes.

O Marco Civil reconhece à internet como essencial ao exercício da cidadania, assegurando além de outros direitos ao usuário a manutenção da qualidade contratada da conexão à internet. O artigo 9º impõe ao provedor de acesso o "dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço,

terminal ou aplicativo". O principal objetivo do artigo é evitar que haja discriminação ou privilégios no tratamento dado aos provedores de conteúdo.

O artigo 10 prevê a guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet, que devem atender à preservação da intimidade, a privacidade, a honra e a imagem das partes direta ou indiretamente envolvidas. O artigo 13 descreve sobre a provisão da conexão da internet, e os registros de conexão que devem estar disponíveis mesmo que sob sigilo durante um ano. Já no artigo 11, é descrito sobre a guarda de informações pertinentes ao conteúdo acessado pelo usuário como responsabilidade de um todo, mas, principalmente, dos provedores de acesso.

A não responsabilidade sobre possíveis danos causados por terceiros está previsto no artigo 19, que descreve que " o provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros, assegurando a liberdade de expressão e impedindo a censura, podendo ser responsabilizado somente após ordem judicial específica que não seja tomada determinadas providências, como exclusão do conteúdo apontado como infringente, com ressalvas as disposições legais em contrário.

O artigo 21 versa sobre a "pornografia de vingança", estabelecendo que o provedor de internet que disponibilizar conteúdo gerado por terceiros será responsabilizado de maneira subsidiária pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, com uso de imagens, vídeos ou outros materiais que possam conter cenas de nudez ou de atos sexuais de caráter privado. Essa responsabilização será gerada quando após o participante ou representante legal receber notificação, deixar de promover de forma diligente a indisponibilização do conteúdo.

De acordo com o exposto, o Marco Civil da Internet possui um tripé axiológico diante a neutralidade da rede, garantindo a privacidade e a liberdade de expressão. A neutralidade está baseada na forma com o que tudo que está presente na rede irá ser transportado, sem discriminações quanto à natureza do conteúdo ou à identidade do usuário, salvo infrações cometidas que já são previstas em lei.

O Marco Civil da Internet se tornou um dos princípios essenciais para a disciplina acerca do uso da internet no Brasil diante a liberdade de expressão, a privacidade e a neutralidade da rede. Apesar do mesmo versar sobre certos pontos da liberdade de expressão, a Constituição Federal de 1988 não parece ter estabelecido uma ponderação acerca de qualquer direito fundamental em específico, mas acaba direcionando maneiras de interpretação que posam garantir uma maior tutela à dignidade da pessoa humana, com cada caso devendo ser analisado de maneira singular.

Por fim, o legislador entendeu que os provedores possuem a possibilidade e o dever de contribuir com a segurança dos usuários, retirando conteúdos que possam ser considerados lesivos quando forem solicitados a fazerem. No ano de 2021 o Presidente da República propôs um PL para garantir direitos dos usuários de rede, promovendo alterações no Marco Civil da Internet. A Proposta de Lei visa a moderação do conteúdo de rede sociais com mais de dez milhões de usuário no Brasil, de modo que não implique em um indevido cerceamento dos direitos e garantias fundamentais.

São acrescidos dispositivos que garantem o direito a informações clara, públicas e objetivas sobre quaisquer políticas e procedimentos de medidas que são utilizadas para moderação de determinados conteúdos, direito ao exercício do contraditório, ampla defesa e recurso nas hipóteses de moderação de conteúdo pelo provedor de rede social. Prevê também o direito a restituição de conteúdo disponibilizado pelo usuário na rede social e exigência de justa causa nos casos de cancelamento ou suspensão de uso de perfis. Outrossim, o provedor de redes sociais é obrigado a notificar o usuário, identificando qual medida irá ser adotada, apresentando a motivação de tal decisão e informação sobre prazos e procedimentos diante a contestação e a eventual revisão da decisão.

3.4.2 Lei Geral de Proteção de Dados (Lei 13.709/2018)

A Lei Geral de Proteção de dados é a lei brasileira mais atual que rege sobre os dados coletados e como os mesmos serão tratados, a mesma entrou em vigor em agosto de 2020. A lei 13.709/2018 protege os direitos fundamentais, como o direito de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural diante a forma que ocorrerá o tratamento de dados.

Em seu artigo 1º descreve sobre o tratamento de dados pessoais, sendo por meio digital ou não, de pessoa natural ou jurídica de direito público ou privado. Esse artigo busca a proteção de direitos fundamentais, como a liberdade e a privacidade. Já no artigo 2º, é apresentado os fundamentos de maneira geral de como irá funcionar a proteção relacionada ao respeito a privacidade, a autodeterminação afirmativa, a liberdade de expressão, a honra e a imagem, informação e comunicação, entre outros.

No artigo 6º é apresentado dez princípios que versam sobre o tratamento de dados. O princípio da finalidade exige que o tratamento de dados seja legítimo, específicos e explícitos, com a informação do titular do dado, e tratamento ilegal quando compatível. O princípio da adequação determina que além da comunicação com o titular, deverá ser garantido que os

limites estipulados pelo mesmo sejam garantidos. O princípio da necessidade define que os dados devem possuir um limite necessário para o cumprimento de sua finalidade, impedindo coletas de dados desnecessárias que não possuem relação com a finalidade. O princípio do livre acesso garante ao titular do dado consulta gratuita e facilitada sobre qualquer atividade que possa envolver seus dados, podendo ser consultada a qualquer momento, pois os dados devem ficar armazenados de maneira que seja possível o livre acesso, esse último princípio está explicito no artigo 9º e no artigo 18 da LGPD. O princípio da qualidade de dados garante a exatidão e clareza diante a atualização dos dados tratados, podendo o titular solicitar revisão de decisões tomadas. O princípio da transparência garante ao titular do dado que as informações sejam precisas e claras, com acesso livre e irrestrito sobre todos os seus dados, limitando a transparência apenas em casos de segredos industriais e comerciais que podem impedir a divulgação de informações. O princípio da segurança descreve que os agentes de tratamento devem utilizar os meios técnicos mais atuais e eficazes para a proteção de dados, sendo digitais ou não. O princípio da prevenção impõe ao agente a obrigação de utilizar medidas de maneira preventiva para que não ocorra dano aos dados. O princípio da não discriminação impede que os dados sejam usados para qualquer tipo de discriminação, para ato ilícito ou abusivo. Por fim, o princípio da responsabilização versa sobre o modo que o agente de tratamento deverá atestar que está utilizando as medidas capazes e necessárias para a proteção 42 da Lei está descrito as sanções administrativas que o mesmo pode sofrer.

De acordo com o exposto acima, Demócrito Reinaldo Filho (2018) descreve sobre a importância da LGPD para o Brasil para ocasiões que aconteciam anteriormente a mesma.

> O Brasil vinha perdendo oportunidades de investimento financeiro internacional em razão do "isolamento jurídico" por não dispor de uma lei geral de proteção de dados pessoais. A União Europeia, por exemplo, veda a transferência de dados de cidadãos europeus para empresas de outros países que não têm um "nível adequado" de proteção de dados pessoais, e o Brasil até então era enquadrado na categoria das nações que não protege de maneira satisfatória a privacidade e intimidade das pessoas.

Ademais, o Marco Civil da Internet (Lei 12.965/14) prevê a segurança dos dados no ambiente online. Já a Lei Geral de Proteção de Dados (Lei 13.709/2018) cria diretrizes severas em relação a aplicação e segurança. Detalhando os tipos de dados existentes e assegurando a movimentação dos mesmos, tanto online, quanto offline.

CONSIDERAÇÕES FINAIS

Com o advento da rede mundial de computadores se faz necessário debater o quão relevante tem se tornado a segurança no meio eletrônico, visto que a expansão tecnológica evidência a dependência das ferramentas virtuais a cada dia, com essa rápida evolução surge múltiplas espécies de infrações eletrônicas. Esses delitos demandam alerta de todos os usuários da rede, tanto da sociedade civil, quanto de todos os poderes do Estado, sendo evidente a importância que a internet possui no cotidiano de todos os indivíduos, há a necessidade de estudos e pesquisas que aprofundem a origem desses delitos e modos do usuário se portar no ambiente eletrônico, para que a legislação consiga se atualizar na velocidade que surgem esses crimes.

A proteção de dados está intrinsecamente relacionada a dignidade humana, liberdade e privacidade, portanto não se deve aceitar o rompimento desses preceitos, os dados são inteiramente de posse do usuário, qualquer compartilhamento ou exposição deverá ser consentida pelo mesmo. O avanço tecnológico e de como ele se relaciona com o cotidiano dos indivíduos, cria-se cidadãos globalizados e interligados, com acesso contínuo que acaba gerando hábitos e situações que faz, com que a cada nova conexão a sua privacidade e a proteção de seus dados seja colocada em risco

Portanto, para resguardar esses direitos fundamentais dos usuários e que possam interagir nos meios eletrônicos sem grandes percalços, é de suma importância que se garanta a sua privacidade e a segurança dos seus dados pessoais, fica a cargo de sites, aplicativos e provedores de internet efetivarem o uso correto e ético das informações por eles coletadas. Sendo imputada ao direito, com a partição direta da sociedade civil e também do Estado a responsabilidade de um futuro justo para a rede e todos que a utilizarem.

O Marco Civil da Internet se transformou em uma das principais normas que disciplinam e normatizam o uso da rede no Brasil, com foco na neutralidade da internet, privacidade e na liberdade de expressão. Reforçando o texto da Constituição Federal de 1988 dos direitos fundamentais em específico a liberdade de expressão, e também dando direção a modos de se interpretar, para que se garanta a preservação da dignidade da pessoa. Com cada situação sendo apreciada de maneira individual.

Por conseguinte, por entendimento dos legisladores, os provedores, dispõe da viabilidade e a obrigação de colaborar com a segurança dos indivíduos que utilizam a rede, removendo retirando publicações que possuem caráter lesivo quando for solicita a retirada.

É perceptível que desde a democratização da internet, o uso e a absorção de dados pessoais ultrapassam as barreiras legais de tratamento da privacidade dos usuários. A criação de normas era extremamente imprescindível para se resguardar os dados e por consequência a privacidade na sociedade globalizada. A Lei Geral de Proteção de Dados foi legislada para ser uma solução desses percalços. O tratamento justo dos dados permite inúmeras situações comerciais e aperfeiçoam o funcionamento do sistema, reduzindo as chances de problemas com segurança e aumentando a circulação protegida de dados de bens e serviços, criando a possibilidade de um crescimento exponencial da tecnologia. Outrossim, existe a vantagem da utilização do Estado desses dados, para a segurança Nacional e de segurança pública, com o objetivo de investigações em situações criminais e no combate a delitos.

REFERÊNCIAS

ABREU, Karen Cristina Kraemer. **História e usos da Internet**. Biblioteca on-line de ciências da comunicação, 2019. Disponível em: http://www.bocc.ubi.pt/_esp/autor.php?codautor=1625. Acesso em: 05 de set. 2021.

AGUIAR, Vanessa. **A Transformação Digital no governo e órgãos públicos**. 2018. Disponível em: < https://transformacaodigital.com/transformacao-digital-nogoverno-e-orgaos-publicos/>. Acesso em: 09 out. 2021.

ALECRIM, Emerson. **O que é Internet das Coisas (Internet of Things)?** Disponível em https://www.infowester.com/iot.php . 2016. Acesso em 14. Set .2021

BARRETO, Alesandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de Investigação Cibernética à luz do Marco Civil da Internet**. Rio de Janeiro: Brasport, 2016. P. 222

BORGES, Fabiani. **Terrorismo Cibernético e a Proteção de Dados Pessoais**. 2015. Disponível em: http://ebqadvogados.com.br/terrorismo-cibernetico-e-a-protecao-de-dados-pessoais/ . Acesso em: 08 out. 2021. BRASIL.

CERT.BR: **Estatísticas**. 2017. Disponível em: https://www.cert.br/stats/incidentes/2017-jan-dec/analise.html#:~:text=O%20total%20de%20notifica%C3%A7%C3%B5es%20recebidas,que%20o%20total%20de%202016.. Acesso em: 05 ago. 2021.

CGI. Comitê Gestor Internet (Org.). **Recomendações para o Desenvolvimento e Operação da Internet no Brasil.** Disponível em: https://www.cg.org.br/recomendacoes-para-o-desenvolvimento-e-operacao-da-internet-no-brasil/ . Acesso em: 08 jul. 2021

CONCERINO, Arthur José**. Internet e segurança são compatíveis?** Arthur José Concerino. Newton de Luccas e Adalberto Simão Filho. (coord.) Direito & Internet: aspectos jurídicos relevantes. Edipro 2001, p. 153

COSTA, Júlio Rezende**. Ferramentas de escrita colaborativa da Web 2.0 e mediação pedagógica por computador: construção e ressignificação do conhecimento on-line**. In: Simpósio Internacional a Distância, 2012, São Carlos. Anais eletrônicos... São Carlos: Universidade Federal de São Carlos, 2012. Disponível em: http://sistemas3.sead.ufscar.br/ojs/Trabalhos/20-900-1-ED.pdf. Acesso: 27 mar. 2021

COUTINHO, Clara Pereira; BOTTENTUIT Junior, João Batista. **Blog e Wiki: os futuros professores e as ferramentas da web 2.0.** In: IX Simpósio Internacional de Informática Educativa, 9, 2007 Disponível em : https://core.ac.uk/download/pdf/55608174.pdf. Acesso: 15 jun. 2021

DAMÁSIO DE JESUS apud ARAS, Vladmir. **Crimes de informática: Uma nova criminalidade.** Disponível em https://jus.com.br/artigos/2250/crimes-de-informatica. Acesso em 5 jul. 2021.

FERREIRA, Ivette Senise. **A criminalidade informática**, in: LUCCA, Newton de; SIMÃO FILHO, Adalberto (coord.). **Direito e internet: aspectos jurídicos relevantes**. Bauru: Edipro, 2000.

FERREIRA, Ivette Senise. Direito & Internet: **Aspectos Jurídicos Relevantes**. 2 ed. São Paulo: Quartier Latin , 2005, p.261

FORTES, Vinícius Borges; BOFF, Salete Oro. **A Privacidade e a Proteção dos Dados Pessoais no Ciberespaço como um Direito Fundamental: perspectivas de construção de um marco regulatório para o Brasil.** Sequência: Estudos Jurídicos e Políticos, 2014. Disponível em: https://www.scielo.br/j/seq/a/LqY93YW8FMSNPgkVBg75nbH/abstract/?lang=pt. Acesso em: 05 out. 2021.

LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2011. P.402

MIRABETE, Julio Fabbrini, **Manual de direito penal** - 24. Ed. – São Paulo: Atlas, 2006. p. 134, 135.

NOGUEIRA, Paulo Lúcio, **Em Defesa da Honra**, São Paulo, Saraiva. 1995 p. 116

PRADO, Luiz Regis. **Comentários ao código penal: jurisprudência, conexões lógicas com os vários ramos do direito**. 9. ed., rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2014. 1147 p. ISBN 978-85-203-5177-2

REINALDO FILHO, Demócrito. **Lei de proteção de dados pessoais aproxima o Brasil dos países civilizados.** Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 23, n. 5498, 21 jul. 2018. Disponível em: <https://jus.com.br/artigos/67668>. Acesso em: 09 out. 2021.

ROSA, Fabrizio. **Crimes de Informática**. Campinas: Bookseller, 2002. P. 53.

SILVA, Rita de Cássia Lopes da. **Direito penal e sistema informático**. São Paulo: Revista dos Tribunais, 2003. ISBN: 8520324126

SOUSA, Gonçalo. **Ciberespaço – Espaço Estratégico de Conflito. CIJCI - Segurança da Informação e Direito Constitucional do Ciberespaço**. Revista Cyberlaw by CIJIC – 3ª edição. ISSN 2183-729. Fevereiro de 2017, p. 108-114.