

GABRIELLY DAIANNE ALVES DOS SANTOS

CRIMES VIRTUAIS: tratamento legal e limitações no combate aos crimes cibernéticos

CURSO DE DIREITO – UniEVANGÉLICA

2021

GABRIELLY DAIANNE ALVES DOS SANTOS

CRIMES VIRTUAIS: tratamento legal e limitações no combate aos crimes cibernéticos

Monografia apresentada ao Núcleo de Trabalho de Curso da UniEvangélica, como exigência parcial para a obtenção do grau de bacharel em Direito, sob a orientação do prof. M.e Karla de Souza Oliveira.

ANÁPOLIS – 2021

GABRIELLY DAIANNE ALVES DOS SANTOS

CRIMES VIRTUAIS: tratamento legal e limitações no combate aos crimes cibernéticos

Anápolis, ____ de _____ de 2021

Banca Examinadora

AGRADECIMENTOS

Agradeço primeiramente a Deus, que tem me sustentado com graça e sabedoria para enfrentar os obstáculos e desafios da graduação.

A minha família, que sempre acreditaram no meu potencial e foram meu apoio e alicerce nos dias difíceis.

A minha professora orientadora M.e Karla de Souza Oliveira, por todos os ensinamentos, conselhos e incentivos, que me fizeram seguir avante e chegar até aqui.

Por fim, agradeço a todos que colaboraram para a conclusão deste trabalho, em especial, aos meus amigos que me incentivaram nos momentos de incredulidade e aos professores que sempre nos dedicaram palavras de força e coragem.

Muito obrigada.

RESUMO

A presente pesquisa busca analisar os crimes virtuais em relação ao tratamento legal e as limitações no combate aos crimes cibernéticos. O estudo sobre o tema justifica-se na medida em que a grande maioria da população mundial tem acesso a *internet* e os crimes virtuais têm se tornado cada vez mais frequentes na nossa sociedade. O objetivo da pesquisa é analisar e classificar os crimes virtuais, definir e elencar normas nacionais e internacionais aplicáveis a estes crimes, identificar as limitações no combate e examinar a competência para julgar tais crimes, além disso, apresentar decisões já existentes acerca do tema. O estudo se realizou a partir do método descritivo observacional, com a leitura de obras científicas e artigos por meio eletrônico, dentre tais autores: Fernando Capez, Guilherme de Souza Nucci, Aury Lopes Júnior, Ronaldo Lemos e outros autores citados na pesquisa. Por uma questão didática, a pesquisa se divide em três capítulos. O primeiro trata sobre o histórico da *internet* e sua influência na sociedade, bem como conceitua e classifica as espécies de crimes virtuais, o segundo capítulo apresenta as legislações nacionais e internacionais que refletem no tema, e, por fim, o terceiro capítulo aborda as limitações no combate dos crimes virtuais, além disso apresenta uma reflexão sobre a competência para processar e julgar tais crimes e as decisões dos tribunais existentes no nosso ordenamento jurídico. Logo, a pesquisa abordou relevantes conceitos relacionados ao Direito Penal e a sociedade de informação.

Palavras-chaves: Crime; Virtual; *Internet*; Computador; Ciberespaço.

SUMÁRIO

INTRODUÇÃO	01
CAPÍTULO I – CRIMES VIRTUAIS	03
1.1 Histórico	03
1.2 Conceito e espécies de crimes virtuais	05
1.2.1 – Conceito	05
1.2.2 – Espécies.....	06
1.2.2.1 – Pornografia infantil.....	06
1.2.2.2 – Crimes contra a honra	07
1.2.2.3 – Fraudes Virtuais	08
1.2.2.4 – Crimes contra a propriedade intelectual	08
1.2.2.5 – Estelionato.....	09
1.3 <i>Internet</i> e a vida privada	09
CAPÍTULO II – TRATAMENTO LEGAL	12
2.1 Marco civil da <i>internet</i>	12
2.1.1 – Processo de construção	12
2.1.2 – Fundamentos	13
2.2 Legislação nacional.....	15
2.2.1 – Lei n. 12.737/2012.....	15
2.2.2 – Lei n. 12.735/2012.....	17
2.2.3 – Projetos de Leis.....	18
2.3 Legislação internacional	19
CAPÍTULO III – LIMITAÇÕES AO COMBATE	22
3.1 Provas	22
3.2 Competência	25
3.3 Decisões dos tribunais	26
3.3.1 – Crime de calúnia	27
3.3.2 – Imagens vazadas e a Lei Geral de Proteção de Dados	27
3.3.3 – Comércio online	28
3.3.4 – Extorsão pela <i>internet</i>	29
CONCLUSÃO	30
REFERÊNCIAS.....	32

INTRODUÇÃO

A presente pesquisa tem como objetivo analisar os crimes virtuais abordando o tratamento legal e as limitações no combate a estes crimes. Ademais, evidencia o avanço tecnológico e o advento da *internet* na vida em sociedade, bem como explana as mudanças trazidas por essas tecnologias, especialmente no âmbito penal.

A justificativa para o tema se desenvolve no argumento de que a compreensão a respeito dos crimes virtuais auxilia na reflexão de maneiras de combater, minimizar e neutraliza-los de forma eficaz. Por isso, a importância em conhecer as classificações, buscando identificar quais os crimes virtuais mais praticados e como a legislação trata tais delitos.

A pesquisa foi desenvolvida em três capítulos e a metodologia utilizada é a descritiva observacional, com a leitura de obras científicas e artigos por meio eletrônico. Foi desenvolvida uma pesquisa bibliográfica, utilizando-se como apoio e base contribuições de diversos autores, tais como Fernando Capez, Guilherme de Souza Nucci, Ronaldo Lemos, Augusto Tavares Rosa Marcacini, Damásio de Jesus, José Antônio Milagre e outros.

O primeiro capítulo aborda um breve histórico do surgimento dos computadores, da *internet* e dos crimes virtuais. Ainda nesse tópico é apresentado o conceito e espécies de crimes virtuais, tais como, pornografia infantil, crimes contra a honra, fraudes virtuais, crimes contra a propriedade intelectual e estelionato. Por fim, é tratado a respeito da influência da *internet* na vida privada, bem como os riscos que esta tecnologia traz à privacidade.

O segundo capítulo apresenta as importantes legislações nacionais e internacionais que proporcionaram significativas alterações no Código Penal Brasileiro no sentido de tipificar os crimes praticados no ambiente virtual e adequar alguns artigos já existentes para a realidade cibernética. Além disso, o capítulo também versa sobre o Marco Civil da *Internet*, uma construção democrática e social que visa estabelecer direitos, deveres, princípios e garantias no ciberespaço.

O terceiro capítulo busca explicar as limitações no combate aos crimes virtuais, como a dificuldade de obtenção de provas desses delitos, diante do anonimato possibilitado pelo ambiente virtual, bem como a deficiência de aparatos investigativos capazes de identificar os agentes criminosos. Ademais, observa-se uma reflexão acerca da competência para processar e julgar tais crimes, já que muitas das vezes não é possível identificar ao certo o local de onde a conduta criminosa é praticada. Por fim, é apresentado uma série de decisões existentes no nosso ordenamento jurídico quanto ao tema.

Consigna-se que trata de um tema contemporâneo e corriqueiro. A *internet* tem se tornado o principal meio de comunicação e compartilhamento de informações da sociedade. Sendo o Direito um conjunto de normas jurídicas direcionadas a organizar a sociedade, incumbe a este acompanhar todas mudanças decorrentes da evolução tecnológica e promover novas soluções para os atuais litígios trazidos com as práticas dos crimes cibernéticos.

CAPÍTULO I – CRIMES VIRTUAIS

A compreensão acerca da evolução da tecnologia, do histórico da sociedade de informação e das ameaças virtuais que esses institutos trazem a sociedade atual auxiliam no entendimento quanto aos crimes virtuais, sua conceituação e suas espécies. A relação entre direito, *internet* e a vida privada, além de contemporânea, é necessária para deliberar conflitos no ambiente virtual que se tornam cada vez mais frequentes e corriqueiros, trata-se de um desafio a ser superado, em especial, pelo direito, que é o responsável por sua regulamentação.

1.1 Histórico

A *internet* é um importante canal de pesquisa, de interação e de relacionamento humano, uma criação humana que tem influência sobre grande parte da população mundial e como toda criação humana, pode ser utilizada tanto para o bem, quanto para o mal. Diante da sua essencialidade, o Direito tem despertado crescente interesse por ela e pelas consequências jurídicas que ela produz, conhecer sua evolução é importante para se entender a evolução dos crimes virtuais.

Segundo Zanellato. “A *internet* é um suporte (ou meio) que permite trocar correspondência, arquivo, ideias, comunicar em tempo real, fazer pesquisa documental ou utilizar serviços e comprar produtos” (2002, p.173). Sendo assim, é uma rede em escala mundial, onde armazena dados e informações de milhões de pessoas de todo o mundo.

Embora hoje possa se utilizar da *internet* em celulares, *tablets*, vídeo games entre outros dispositivos, sua invenção está associada ao desenvolvimento dos computadores, que tem sua origem em 1847, com a máquina analítica do

matemático inglês Charlie Babbage, e que foi se desenvolvendo ao longo dos anos e de acordo com a necessidade das pessoas. (OLIVEIRA JÚNIOR, 2001)

Os computadores surgiram para auxiliar em cálculos matemáticos, no entanto se tornaram máquinas, que além de serem suporte para cálculos, possibilitam a realização de pesquisas, comunicação, entretenimento, *home office*, e uma série de atividades que até então, não eram possíveis de serem realizadas.

A *internet* surgiu com objetivos militares, em 1969 criada pela ARPA, uma subdivisão do Departamento de Defesa dos Estados Unidos, ela foi criada como uma rede de dados e informações que estaria espalhada por diversos lugares estratégicos e que não pudessem ser destruídos por bombardeios. Em seguida, ela foi usada pelos estudantes de universidades, a fim de obterem resultados de estudos e pesquisas. (OLIVEIRA JÚNIOR, 2001)

Desde a sua criação, a *web* possui um poder de arma. Ela foi criada por objetivos militares, mas não se sabia que ela se tornaria um canal para criminosos praticarem delitos, uma rede que armazena dados e informações, mas que possibilita que esses dados sejam roubados, alterados ou adulterados. De fato, eles não podem ser destruídos por bombardeios, mas podem ser manipulados.

Na década de 80 a *internet* se tornou o que se conhece hoje, conceituada como um conjunto de redes interligadas podendo ser acessada por todos e com isso trazendo novos conceitos como o de *hacker*, ciberespaço, dentre outros. Desde então muito se discute a respeito da necessidade de regulamentação desse ambiente. (OLIVEIRA JÚNIOR, 2001)

Na opinião de Reginaldo César Pinheiro:

Com a popularização da Internet em todo o mundo, milhares de pessoas começaram a se utilizar deste meio. Contemporaneamente se percebe que nem todos a utilizam de maneira sensata e, acreditando que a internet um espaço livre, acabam por e ceder em suas condutas e criando novas modalidades de delito: os crimes virtuais. (2000, *online*)

Os crimes virtuais tiveram maior evidência de 1960 em diante, principalmente em casos de manipulação e sabotagem de sistemas. Em 1970 a figura do *hacker* já era conhecida em razão dos crimes de invasão e furto de *software*. Em 1980 tais crimes se difundiram com as práticas de invasões de sistema, pirataria,

pedofilia entre outras, sendo necessário maiores preocupações com a segurança virtual. (CARNEIRO, 2012)

Em 1995 o Ministério das Comunicações criou o Comitê Gestor da Internet no Brasil, por meio da Portaria Interministerial nº 147, que tem como atribuições estabelecer diretrizes relacionadas ao uso da *internet* no Brasil e também promover e recomendar procedimentos de segurança. Além disso, inspiraram a proposta legislativa do Marco Civil da Internet, uma lei que regulamenta os direitos e deveres para o uso da *internet*, que será tratado posteriormente. (CGI, s.d.)

1.2 Conceito e espécies de crimes virtuais

1.2.1 conceito

Com o desenvolvimento dos computadores e a difusão da *internet*, tornam-se cada vez mais comuns situações em que pessoas prejudicam outras utilizando-se dessas ferramentas, vez que elas possibilitaram a criação de um espaço público virtual que influencia diretamente na vida pessoal, pública, financeira e coletiva. Surgiram então, pessoas especializadas em informática e tecnologia que praticam crimes por todo o mundo. São os denominados crimes virtuais ou cibernéticos.

Segundo Fernando Capez “O crime pode ser conceituado sob três enfoques, quais sejam, aspecto material, aspecto formal e aspecto analítico” (2020, p. 185). O aspecto material é aquele que está ligado aos bens jurídicos fundamentais e que são de alguma forma lesados ou expostos a algum perigo, o aspecto formal resulta da legislação e da ligação da conduta ao tipo penal e por fim, o aspecto analítico em que crime é todo fato típico e ilícito.

Augusto Rossini conceitua:

[...] 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 a confidencialidade. (2004, p. 110.)

O objetivo não é trazer distinções do universo penal, mas expressar que os crimes virtuais possuem as mesmas características das infrações penais. Assim,

depreende-se como crime virtual a conduta típica e ilícita praticada por meio de um computador e da *internet*. Vale ressaltar que, conforme Rossini, os delitos praticados através de um computador, mesmo que não esteja conectado a *internet*, também são considerados crimes virtuais.

Não há uma legislação que trate o conceito de crimes cibernéticos, nem tão pouco que os classifique, as análises e condenações são feitas a partir do Código Penal Brasileiro. No entanto, alguns autores classificam tais crimes como puros e impuros, sendo os puros as condutas não tipificadas e os impuros os tipos penais já tipificados e que ocorrem no ciberespaço.

1.2.2 *Espécies*

Grande parte dos crimes virtuais também existem no mundo real. Ocorre que, além de se desenvolverem e inovarem muito rápido, em razão do avanço tecnológico, muitas condutas que se espalham na *web* são difíceis de se encontrar o agente que a praticou, vez que ocorrem livremente, não encontram barreiras e possuem o anonimato.

Existem diversas espécies de crimes cibernéticos, Rodrigo Guimarães Colares nos ensina que:

Dessa forma, são crimes que podem admitir sua consecução no meio cibernético: calúnia, difamação, injúria, ameaça, divulgação de segredo, furto, dano, apropriação indébita, estelionato, violação ao direito autoral, escárnio por motivo de religião, favorecimento da prostituição, ato obsceno, escrito ou objeto obsceno, incitação ao crime, apologia de crime ou criminoso, falsa identidade, inserção de dados falsos em sistema de informações, adulteração de dados em sistema de informações, falso testemunho, exercício arbitrário das próprias razões, jogo de azar, crime contra a segurança nacional, preconceito ou discriminação de raça-cor-etnia-etc, pedofilia, crime contra a propriedade industrial, interceptação de comunicações de informática, lavagem de dinheiro e pirataria de software. (2002, *online*)

Neste momento, será abordado, os crimes virtuais impróprios. Dentre esses os mais comuns como: pornografia infantil, crimes contra a honra, fraudes virtuais, crimes contra a propriedade intelectual e estelionato.

1.2.2.1 *Pornografia infantil*

Dentre as denúncias mais comuns de crimes virtuais estão as relacionadas a fraudes e pornografia infantil. O Brasil, ocupa o 4º lugar no ranking mundial de consumo de material relacionado a pedofilia e a pornografia infantil, movimentando grandes operações policiais a fim de combater tal crime, em que pessoas comercializam fotos ou vídeos pornográficos envolvendo crianças e adolescentes. (G1, 2008)

Os artigos 240 e 241 do Estatuto da Criança e do Adolescente tratam acerca da produção e comercialização de material pornográfico. Trata-se da criminalização da conduta de publicar ou divulgar foto ou vídeo de criança e adolescente, inclusive por meio de comunicação, como a internet. Quem guarda esse tipo de material em sites e em computadores também praticam o mesmo delito. Aqui é irrelevante o acesso de usuários, é suficiente para a caracterização do delito a existência de material pornográfico. (BRASIL, 1990)

Conforme Guilherme de Souza Nucci:

A maneira pela qual o autor do crime adquire, possui ou armazena o material é livre, valendo-se o tipo da expressão “por qualquer meio” Comumente, com o avanço da tecnologia e da difusão dos computadores pessoais, dá-se a obtenção de extenso número de fotos e vídeos pela Internet, guardando-se o material no disco rígido do computador, em disquetes, DVDs, CDs, pen drives, entre outros. (2018, p. 849)

Para se encontrar os agentes desses crimes, muita das vezes são necessários a quebra de sigilo e o rastreamento dos computadores onde se encontram tais materiais até que se chegue a quem praticou a conduta ilícita, vez que, na maioria das vezes os criminosos se utilizam do anonimato.

1.2.2.2 Crimes contra a honra

A inviolabilidade da honra é direito fundamental protegido pela Constituição Federal em seu artigo 5º, inciso X. A honra é um patrimônio pessoal, está relacionada a qualidades físicas, morais e intelectuais de uma pessoa e sua proteção se justifica, vez que está diretamente relacionada com o respeito, a aceitação e bom convívio social em um determinado grupo. (BRASIL, 1988)

Por ser um crime virtual impróprio, tais tipos penais já estão previstos nos artigos 138, 139 e 140 do Código Penal, sendo os mesmos crimes comuns, só que

praticados através da internet. Trata-se da conduta de caluniar, difamar ou injuriar alguém, principalmente imputando-lhe fato ofensivo a sua reputação ou ofendendo-lhe a dignidade. (BRASIL, 1940)

Nesses crimes, os agentes se utilizam de diversos meios virtuais para a prática do crime, como o e-mail e as redes sociais. Esse tipo de crime cresce muito no meio social, em razão de ódio gratuito, inveja, preconceitos ligados a gênero, cor e religião, em especial nas redes sociais que ganharam muita força nos últimos tempos. Ressalta-se que também são crimes, onde o agente, normalmente se utiliza do anonimato para praticá-los, tornado mais difícil o seu reconhecimento.

1.2.2.3 *Fraudes virtuais*

O crime de fraude virtual ocorre quando o agente invade, altera, modifica, ou adultera dados eletrônicos, programas ou um sistema de processamento de dados, por exemplo, quando alguém invade o computador de outra pessoa e divulga fotos íntimas no ambiente virtual.

Paulo Marco Ferreira Lima, define as fraudes virtuais como:

Fraudes virtuais-é uma invasão de sistemas computadorizados e posterior modificação de dados, que tem como intuito do obter vantagem sobre bens, física ou não, ou seja, a adulteração de depósitos bancários, aprovações em universidades, resultados de balanços financeiros, pesquisas eleitorais, entre outros. (2005, p. 60)

Nas fraudes, os usuários são induzidos de forma mascarada a fornecerem seus dados pessoais e financeiros, por meio de páginas, *links*, propagandas, mensagens, fraudulentas através das mídias sociais. É uma ação intencional com o objetivo de alcançar um benefício, satisfação psicológica, financeira ou material.

Dentre as principais fraudes virtuais, estão o *phishing* quando os criminosos enganam a vítima para obterem informações pessoais, como CPF, cartão de crédito e senhas, por e-mail ou por um *website* falso e as promoções falsas via *WhatsApp*, que normalmente são anúncios atrativos, mas que na verdade, são meios de obter dados da vítima. As fraudes via *WhatsApp* se tornam cada vez mais comuns, vez que o aplicativo é uma ferramenta utilizada por diversas pessoas.

1.2.2.4 *Crimes contra a propriedade intelectual*

A propriedade intelectual é a esfera do direito que busca resguardar aos inventores e responsáveis por produções intelectuais o direito de serem recompensados e reconhecidos por suas criações. (VANIN, 2016)

O ambiente virtual possibilita uma rápida circulação de informações, inclusive cópias de trabalhos e obras feitos fora de ordem por outras pessoas, sem que haja qualquer apoio aos direitos do autor da obra verdadeira. A ausência de fiscalização também corrobora para que esse delito seja praticado, vez que não há um controle. Além das cópias de obras também é comum a pirataria de *software* e de aplicativos através da *internet*.

Hoje em dia, se tem a ideia de que tudo o que está na *internet* é público, no entanto a propriedade intelectual é um direito, protegido por lei a pessoa que criou determinada obra, cabendo a ela, usufruir dos benefícios e da exclusividade do objeto de seu intelecto.

1.2.2.5 Estelionato

Outro crime que se tornou popular com o avanço tecnológico é o estelionato. O artigo 171 do Código Penal, estabelece como estelionato a conduta de 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.

Entende Rogério Greco no seguinte sentido:

Desde que surgiram as relações sociais, o homem se vale da fraude para dissimular seus verdadeiros sentimentos e intenções para, de alguma forma, ocultar ou falsear a verdade, a fim de obter vantagens que, em tese, lhe seriam indevidas. (2014, p. 236)

No ambiente virtual a conduta do estelionatário será de tirar vantagem ilícita para si ou para outrem, induzindo ou mantendo a vítima em erro. Encaminhar *e-mails* falsos, levando o usuário a clicar em links que o direciona a um site falso com o objetivo de apropriar-se dos seus dados bancários para adquirir para si os valores na conta da vítima é constituído como uma das condutas de estelionato virtual.

1.3 *Internet* e a vida privada

A tecnologia da informação influencia e modifica todas as esferas do cotidiano do homem, inclusive a vida privada, que se torna cada vez mais exposta aos holofotes da internet. Nessa perspectiva encontra-se o cidadão comum, que desperta em um universo, onde não se tem mais domínio dos dados pessoais, nem das informações ao seu respeito, o próprio titular não tem controle sobre sua vida privada.

A Constituição Federal resguarda a vida privada e assegura a sua inviolabilidade. Conforme Liliana Minardi Paesani 'O direito à privacidade ou direito ao resguardo tem como fundamento a defesa da personalidade humana contra injunções ou intromissões alheias' (2014, p. 34). Sendo assim, é compreensível que exista um limite entre a esfera da privacidade e o direito à informação.

Apesar da privacidade ser colocada como uma aspiração individual, trata-se de um valor social, um elemento fundamental para a organização da sociedade, vez que tem relevância em toda a sociedade e está entrelaçada com a dignidade da pessoa humana. Portanto, ao protegê-la o Estado busca a manutenção de uma vida digna, onde há liberdade e autonomia.

Para Paesani:

O desenvolvimento da informática colocou em crise o conceito de privacidade- de, e, a partir dos anos 80, passamos a ter um novo conceito de privacidade que corresponde ao direito que toda pessoa tem de dispor com exclusividade sobre as próprias informações mesmo quando disponíveis em bancos de dados. (2014, p. 35)

A tecnologia tem contribuído com a ameaça a privacidade, na medida em que possibilita a invasão na intimidade das pessoas. A *internet* comercializa as informações, além de acumular dados em quantidade ilimitada, seja elas físicas, mentais, econômicas, opiniões religiosas ou políticas, também possibilita o confronto das informações obtidas.

As redes sociais, que ganharam grande força ao longo dos anos, possibilitam a exposição da privacidade, vez que as pessoas publicam fotos, sentimentos, opiniões e se desnudam ao expor características e experiências íntimas, além disso, por meio delas, criam-se comunidades entre usuários com interesses comuns. Vale ressaltar que essas informações podem ser utilizadas livremente por qualquer um.

A violação da vida privada ocorre devido a falta de regulamentação através de leis e também devido a dificuldade de limitar e acompanhar os acessos, além disso muitos usuários não conhecem o limite entre a liberdade de expressão e o respeito ao outro e deslocam dados de um ambiente virtual privado para um ambiente público.

No entendimento de Victor Drummond, são critérios que separam a esfera pública da esfera privada no ambiente virtual:

- a) identificação do destinatário da mensagem: a mensagem cujo destinatário for indeterminado será uma mensagem pública, já a mensagem cujo destinatário for determinado poderá ser pública ou privada, dependendo dos demais critérios;
- b) ciência das demais pessoas envolvidas na comunicação: a mensagem será privada se o emissor tiver conhecimento das pessoas envolvidas na comunicação e será pública se não tiver conhecimento dos destinatários;
- c) existência de intimidade entre os interlocutores: a mensagem será privada se o grupo for coeso e formado por amigos ou pessoas que tenham qualquer outra estreita relação, a mensagem será pública se o grupo for formado por pelo menos um estranho. (2003, p. 27)

É sabido que nem toda divulgação de informações acerca da vida privada é ilícito, pois as vezes as próprias pessoas expõem dados pessoais com algum intuito. Ocorre que, esses dados não podem ser repassados adiante com o interesse de humilhar ou depreciar a honra da pessoa. Nesse prisma José Miguel Garcia Medina coloca “A constituição também protege a imagem. A honra de uma pessoa pode ser atingida quando indevidamente usada sua imagem, bem como, p.ex. em face do mau uso do seu nome [...]” (2014, p. 85).

Com a invasão da *internet* à vida privada estão em risco as contas correntes, números de cartões de crédito, nomes e endereços, contatos comerciais e pessoais, disponíveis em qualquer lugar do mundo. E o mais grave é que esses dados podem ser alterados, será um crime, porém de difícil apuração e punição. Essa ameaça vem de um lado negro do avanço tecnológico.

Por isso, a importância da conscientização dos internautas em relação aos riscos que a rede pode causar à privacidade, para que o usuário se proteja de programas duvidosos e utilize o computador e a *web* de forma mais segura, sem exagerar na auto exposição para se sentirem digitalmente incluídos.

CAPÍTULO II – TRATAMENTO LEGAL

O ambiente virtual e sua constante expansão impõe o grande desafio aos legisladores de conceituar, tipificar e criminalizar as práticas delituosas cometidas no âmbito virtual. Embora seja uma realidade consideravelmente recente, já é possível observar uma constante movimentação legislativa, no sentido de regulamentar o ambiente virtual e combater determinados crimes, não só no Brasil como também internacionalmente, uma vez que trata-se de uma temática global.

1.1 Marco civil da *internet*

O marco civil da *internet* surgiu para regulamentar questões relacionadas a internet, estabelecendo direitos, deveres princípios e garantias com o fito de consolidar avanços significativos em relação ao ambiente virtual. É uma construção democrática e social, pois durante seu processo de criação, a sociedade participou ativamente, tornando-se um verdadeiro marco civil e social.

1.1.1 *Processo de construção*

A elaboração do projeto de lei que resultaria no Marco Civil, foi dividida em duas partes, sendo a primeira um debate de princípios que norteariam todo o projeto e a partir desses princípios fundamentais e a a segunda fase que concretizava tais princípios, sendo efetivamente a construção do texto legal. Ronaldo Lemos ressalta que “O Marco Civil deveria promover a liberdade de expressão, a privacidade, a neutralidade da rede, o direito de acesso à internet, os limites à responsabilidade dos intermediários e a defesa da abertura (*openness*) da rede, crucial para a inovação.” (LEMOS, *et al*, 2014, p. 5)

Ronaldo Lemos ainda salienta:

Com isso, ao dar um passo no sentido de regulamentar essa questão o Marco Civil atende a dois princípios importantes. O primeiro de fortalecer o princípio da liberdade de expressão, protegendo em alguma medida os intermediários da informação. Em segundo lugar, impulsiona a inovação local, na medida em que permite a jovens empreendedores brasileiros saberem de antemão os limites da sua responsabilidade, gerando previsibilidade e alavancando o surgimento de novos serviços baseados no país. (2014, p. 6)

Sendo um objeto de preocupação social, a participação popular ocorreu através debates abertos e coletivos, o texto legal foi posto em plataformas de debates públicos e além de comentários e opiniões formais. Também levou-se em consideração outras formas de contribuição em redes sociais como o *twitter* e em *posts* e *blogs*. (LEMOS, *et al*, 2014)

Então em 23 de abril de 2014 foi sancionada a Lei nº 12.965, uma conquista social e democrática, uma inovação em relação a uma nova metodologia de construção legislativa, um avanço para uma sociedade cada vez mais digital, um resultado de longos debates, uma construção coletiva e uma resposta para questões pró-inovação e pró-direitos no âmbito virtual.

1.1.2 Fundamentos

O Marco civil da *internet* possui três pilares fundamentais, sendo eles: a garantia da neutralidade da rede; a garantia da liberdade de expressão e comunicação; e a privacidade dos usuários e proteção de seus dados. Trata-se de relevantes princípios diante de um poderoso ambiente, onde preocupa-se com os dados pessoais que são disponibilizados, com os provedores que irão receber esses dados e ainda há uma preocupação de não suprimir um direito constitucional diante de regras de prevenção e proteção. (AKCHAR, 2017)

A neutralidade da rede diz respeito a preservação da liberdade que a internet proporciona aos usuários, é um tema fundamental e igualmente polêmico. Presente no artigo 9º do Marco Civil da *Internet*, ele garante que os pacotes de dados devem receber um tratamento isonômico, o que significa que há uma proibição de que tais pacotes sejam discriminados na rede onde são roteados. (BRASIL, 2014)

O interesse despertado pela *internet* está na disponibilidade do acesso, por qualquer pessoa, sua valoração está no vasto banco de informações que ela permite acessar e na possibilidade de estabelecer comunicação com qualquer lugar do planeta, portanto, não parece razoável que alguém possa se apropriar dessa rede colocando em detrimento interesse alheio.

Marcacini, exemplifica:

Comparada a Internet à malha viária de uma cidade, imagine-se pequenos caminhõezinhos (os pacotes de dados) saindo carregados de informação de um endereço a outro, cada qual desses veículos eventualmente tomando um rumo diferente pelas muitas ruas e avenidas e, a cada esquina, o motorista pergunte a uma autoridade de trânsito (que aqui representa o roteador) qual o melhor caminho para o endereço de destino. Segundo a lei, não caberia a esse sujeito do exemplo bloquear ou retardar a passagem do caminhão, com base no tipo, origem ou destino da carga transportada: deve, isto sim, dar prontamente a informação sobre a direção a seguir e liberar sua passagem, sem preferir ou preterir quaisquer dos caminhões que passam por ali. (2016, p. 42)

Ao estabelecer o tratamento isonômico aos pacotes de dados, isso assegura que a *internet* seja um canal universal de comunicação, preserva a livre concorrência, a liberdade dos usuários e impede o abuso de poder. Sem a neutralidade da rede, poderia haver por parte dos provedores uma discriminação de determinados conteúdos ou até mesmo um bloqueio, impedindo que os mesmos chegassem até o usuário.

Salienta-se que o Marco Civil da *Internet*, não ficou restrito a afirmação de princípios gerais, há também, regras concretas relacionadas à preservação da privacidade, sendo um dos temas mais tratado na lei. Além disso, orienta a atuação das empresas sobre o que fazer nesse ambiente, responsabiliza os prestadores e dispõe acerca da proteção da privacidade dos usuários.

O art. 3º da lei destaca a proteção da privacidade e a proteção dos dados pessoais, o art. 7º enumera direitos dos usuários e o art. 8º contém normas voltadas a nulidade das cláusulas contratuais que impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas na *internet*, esses são alguns exemplos de normas contidas no Marco Civil com o fito de proteger os usuários e sua privacidade. (BRASIL, 2014)

Por fim, a liberdade e expressão é uma garantia também prevista na Constituição Federal de 1988, em seu art. 5º inciso IV, inciso XIV e no artigo 220, que preveem, respectivamente a livre manifestação do pensamento, o acesso a informação e a manifestação do pensamento, a criação e a informação, com ressalvas em relação ao anonimato, ao resguardo do sigilo e as demais garantias também dispostas na própria Constituição. (BRASIL, 1988)

Segundo Paulo Gustavo Gonet Branco, a liberdade de expressão é:

Toda opinião, convicção, comentário, avaliação ou julgamento sobre qualquer assunto ou sobre qualquer pessoa, envolvendo tema de interesse público, ou não, de importância e de valor, ou não – até porque diferenciar entre opiniões valiosas ou sem valor é uma contradição num Estado baseado na concepção de uma democracia livre e pluralista. (2011, p. 297)

Embora toda manifestação de opinião exerça algum impacto sobre o outro, a liberdade de expressão não abrange a violência, nem a coação física e moral. Conforme Damásio de Jesus e José Antônio Milagre, a *internet* é livre e democrática, é a garantia da liberdade de expressão, é de extrema importância e tende a sempre prevalecer, desde que não viole direitos de terceiros. (JESUS, MILAGRE, 2014)

A promulgação do Marco Civil da *Internet*, embora não trate especificamente de questões criminais, representa um passo importante para a evolução do tratamento legal acerca de temas relacionados ao ambiente virtual, inclusive na esfera criminal. Certamente esse é apenas um marco, um início de um longo caminho que se percorrerá.

1.2 Legislação nacional

A lei exerce um papel fundamental no ordenamento jurídico. Trata-se de uma concretização de objetivos imprescindíveis para reger a vida em sociedade e possui tamanha importância que o seu resultado adquire independência do ente que a criou. Nesse sentido, faz-se necessário conhecer o histórico, o papel no sistema jurídico e a autonomia das leis, nesse momento, relacionadas aos crimes virtuais.

1.2.1 Lei n. 12.737/2012

A Lei n. 12.737/2012, também conhecida como Lei Carolina Dieckmann, foi sancionada em novembro de 2012. Essa lei surgiu, após um inesperado episódio envolvendo a atriz Carolina Dieckmann, em que várias fotos íntimas da atriz foram divulgadas exposta ao público, em razão da invasão de sua privacidade seguida de extorsão. Tal episódio além de ser amplamente debatido em caráter de urgência, encadeou na referida lei que alterou textos do Código Penal Brasileiro.

Conforme aponta Uchôa, “para ser legítima a tutela penal é necessário que o bem seja ‘digno’ dessa proteção, e que sua lesão ou ameaça efetivamente mereça uma sanção penal” (2009, *online*). No entanto, a problemática que envolvia às novas condutas virtuais eram ilegítimas diante do Direito Penal, e, em razão dessa lacuna na legislação surgiu a Lei n. 12.737/2012. (BRASIL, 2012)

Antes da Lei n. 12.737/2012, existiram outros projetos de lei que visavam combater tais condutas, dentre eles o Projeto de Lei n. 89/2003, que tramitou por mais de 10 anos no Congresso Nacional e desencadeou diversos embates jurídicos e críticas, houve também o Projeto de Lei n. 2793/2011 que visava combater o Projeto de Lei n. 89/2003, vez que acreditava-se que seria mais proveitoso para a sociedade. (ROCHA, 2013)

Tal problemática, teve fim com o episódio supracitado envolvendo a atriz Carolina Dieckmann, pois diante dos fatos ocorridos não havia tipificação legal para amparar os crimes cometidos. A partir desse momento, nasceu a Lei n. 12.737/2012, que ao contrário dos projetos de lei anteriores, traz poucas e eficazes alterações no Código Penal, incriminando condutas tipicamente praticadas no ciberespaço.

Menciona Delmanto, *et al*:

Em boa hora o Legislador acrescentou este art. 154-A ao Código Penal. O avanço tecnológico, que tantas maravilhas e facilidades proporciona, traz também um grande risco de as pessoas terem a sua privacidade violada. São inúmeras as formas com as quais os chamados hackers conseguem acessar a memória de computadores alheios, geralmente por meio da internet. (2016, p. 548)

Foram acrescentados ao Código Penal os artigos 154-A e 154-B que tipificam o crime de invasão de dispositivo de informática, em que o agente comete a conduta de invadir dispositivo informático alheio, mediante violação indevida de mecanismo de

segurança com o fim de obter, adulterar ou destruir dados ou informações sem autorização do titular do dispositivo. (BRASIL, 2012)

Por fim, a citada lei alterou os artigos 266 e 298 do Código Penal, adequando-os para a realidade cibernética. O artigo 266 teve seu título alterado passando a inserir a interrupção quanto aos serviços informáticos, passando a se titular "*Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública*" e no parágrafo único do artigo 298 o legislador equiparou o cartão de crédito ou débito ao documento particular no crime de Falsificação de documento particular. (BRASIL, 2012)

1.2.2 Lei n. 12.735/2012

Em 2012, foi sancionada também a Lei n. 12.735, conhecida como Lei Azeredo que teve origem no projeto de lei n. 1999 (PL 84/99). Essa lei visa a tipificação de condutas realizadas através do uso sistema eletrônico, digital ou similares e que seja praticas contra sistemas informatizados. Assim, como a Lei n.12.737/2012, esta surgiu em um momento em que os crimes virtuais ocorreram com mais frequência. (BRASIL, 2012)

A importância de elaboração de leis específicas à internet, está no princípio da legalidade quando a sua taxatividade, como menciona Delmanto:

As leis que definem crimes devem ser precisas, marcando exatamente a conduta que objetivam punir. Assim, em nome do princípio da legalidade, não podem ser aceitas leis vagas ou imprecisas, que não deixam perfeitamente delimitado o comportamento que pretendem incriminar - os chamados tipos penais abertos. Por outro lado, ao juiz que vai aplicar leis penais é proibido o emprego da analogia ou da interpretação com efeitos extensivos para incriminar algum fato ou tornar mais severa sua punição. As eventuais falhas da lei incriminadora não podem ser preenchidas pelo juiz, pois é vedado a este completar o trabalho do legislador para punir alguém. (2002, p. 04)

A partir disso, é possível refletir que para que uma lei específica para o ambiente virtual seja aplicada, não depende apenas da frequente ocorrência das condutas, ou que o magistrado faça uma interpretação análoga ou extensiva, é necessário a previsão normativa do caso concreto e manutenção da ordem jurídica

precisa estar presente também na internet, como está presente nas diversas relações da sociedade.

1.2.2.3 *Projetos de leis*

Diante da importância da tipificação penal acerca de crimes cibernéticos, existem também os projetos de lei que tramitam no nosso cenário legislativo, representando uma possibilidade de serem aprovados um dia e trazerem outras modificações no Código Penal. O crescente desenvolvimento tecnológico e o uso massificado da rede tem impulsionado as casas legislativas a se debruçarem cada vez mais sobre esse assunto.

Nesse sentido:

Seria um grande avanço se fosse elaborado um novo código especificando crimes virtuais, adentrando em todos seus aspectos e criando uma área policial especializada no assunto, com nível de conhecimento em computadores avançado para que possa se resolver o conflito de forma mais habilidosa, facilitando o encontro do criminoso virtual. Nota-se que o sistema jurídico não está totalmente preparado para coibir tais condutas, portanto se as normas que tratam de determinado assunto fossem, talvez, aperfeiçoadas, poderíamos ter a esperança de que os índices de criminalidade virtual reduziram devido a eficácia de suas respectivas leis. (SIQUEIRA, *et al*, 2017, p. 128)

Em um mundo caracterizado pela acelerada adaptação social e inovação tecnológica, onde quase que diariamente surgem novas formas de convivência, convívio e interação coletiva, inclusive na ceara jurídica e judicial, que atualmente, principalmente em razão do Covid-19 está desenvolvendo vastas transformações na forma dos atos processuais em que o remoto se torna cada vez mais frequente, a normatização específica de crimes virtuais e de um aparato policial especializado seria, realmente, um avanço gigantesco.

Dentre os projetos de lei em trâmite, consta o projeto de Lei nº 4287 de 2019 que altera os artigos 141 e 154-A do Código Penal, acrescentando hipóteses de agravamento da pena nos crimes contra a honra praticados usando a *internet* e tipifica a conduta de invadir dispositivo informático, como a conduta de obter, adulterar ou destruir dados sem autorização do usuário do dispositivo. (SENADO FEDERAL, s.d.)

Outra inovação é trazida pelo Projeto de lei n. 4.161/2020 que também altera o Código Penal que determina o agravamento da pena no crime de estelionato e fraude, quando forem praticados na *internet*. Esse projeto foi apresentado pelo Senador Marcos do Val (Podemos-ES) e reflete o recente cenário do isolamento social, causado pelo Covid-19, vez que, em razão disso houve acréscimos das fraudes efetuadas pela *internet*. (SENADO FEDERAL. s.d.)

Por fim, o Projeto de Lei n. 154/19, que também altera o Código Penal e agrava a pena aplicada a quem comete crimes cibernéticos, conforme o texto a agravante será aplicada quando o crime for praticado por meio de computador ou outro dispositivo compatível. A proposta foi aprovada pelo CNJ e segue para análise do Plenário da Câmara dos Deputados. (CÂMARA DOS DEPUTADOS, 2019)

1.3 Legislação internacional

A prática de ilícitos penais virtuais não é uma realidade específica brasileira, na verdade, trata-se uma discussão universal e que necessita de uma cooperação internacional. Diante da complexidade dos fatos apresentados no primeiro capítulo e do elevado potencial de lesividade tais como a perda de privacidade, o anonimato do infrator, a facilidade de propagação e a transnacionalidade desses crimes, tratar esse tipo de criminalidade é essencial para a segurança global das sociedades.

Preceitua Cláudia Perrone Moisés:

Seguindo a tradição de Nuremberg, o direito internacional penal pode ser qualificado, primeiramente, como um direito que protege interesses fundamentais e bens supremos, como a paz e a dignidade do ser humano. Assim, os delitos regulados por ele são atos que violam a ordem pública internacional, por meio de infrações contra o direito internacional. São infrações que interessam ao conjunto da comunidade internacional, por atingirem valores considerados fundamentais para todos os Estados. (2012, p.6)

Nesse sentido, pode-se dizer que os crimes virtuais podem ser resguardados pelo direito penal internacional, pois são atos que violam a ordem pública internacional, na medida que extrapolam os limites territoriais atingindo valores fundamentais para os Estados e colocando em risco o ordenamento jurídico mundial.

A *web* não se limita a países específicos, ela ocorre em escala mundial, portanto, é necessário, também, uma normatização global.

A Convenção de Budapeste sobre o Cibercrime, assinada em 2001, inovou na forma de cooperação penal e regulamentou além da jurisdição nacional, visando combater de forma mais eficiente infrações relacionadas aos cibercrimes. Tal Convenção foi assinada por 43 países e é considerada uma referência legislativa mundial acerca de crimes na *web*. (CÂMARA DOS DEPUTADOS, 2011)

Essa significativa Convenção, visa a defesa da sociedade internacional, adotando uma legislação e promovendo cooperação internacional. A citada Convenção abrange fraudes informáticas, violações de direito autoral, pornografia infantil e invasões de computadores, além disso, estipula uma série de procedimentos entre os países. (ALMEIDA, 2015)

Nesse sentido, conforme Delmanto, citado por Jéssica Lopes:

Dessa forma, a Convenção de Budapeste sobre o Cibercrime se traduz em importante marco para a cooperação penal internacional, tendo em vista a promoção de medidas de aprimoramento de ferramentas de auxílio mútuo e de produção de provas, bem como o implemento de mecanismos de preservação dos elementos probatórios em forma de dados e a celeridade nas investigações e processos penais por meio da divulgação expedita de dados de tráfego preservados, com vista a atender de forma mais eficaz à persecução penal para combate às manifestações da criminalidade informática, que antes não existiam. (*Apud*, s.d., p.28)

A elaboração de tratado e convenções internacionais em matéria penal, em especial relacionados aos crimes virtuais, possibilita integração entre países com o intuito de elaboração de normas eficazes de repressão aos crimes. No entanto, mesmo diante da característica transacional dos cibercrimes, existem mecanismos legislativos e preventivos nacional que devem ser aperfeiçoados e aplicados sobre assunto.

No Brasil, existem órgãos especializados no combate aos cibercrimes, como por exemplo ação conjunta entre Ministério Público Federal, a Polícia Federal e a Organização não governamental Safernet, que recebem e agilizam denúncias relacionadas aos crimes virtuais. Já na esfera estadual, a realidade é outra, poucas Policias Civis têm mecanismos especializados em investigação e combate aos crimes

virtuais, ou seja, os profissionais são despreparados a se compararem com os delinquentes. (WENDT, 2011)

Por fim, além da dificuldade enfrentada no que se refere a legislação e aos órgãos especializados, também surgem muitas dúvidas em relação ao procedimento quando se evidencia a prática do crime virtual. O questionamento do que fazer e como agir quando se é uma vítima de cibercrime é comum no Brasil e isso será tratado no próximo capítulo, assim como as modalidades de provas nesses crimes, que por sinal, também são um obstáculo na obtenção de uma tutela jurisdicional.

CAPÍTULO III – LIMITAÇÕES AO COMBATE

Por tratar-se de uma temática consideravelmente contemporânea e em crescimento esporádico, além das questões legislativas e regulamentais, o tratamento acerca dos crimes virtuais esbarra em outros limites no que se refere ao combate como, por exemplo, a dificuldade de obtenção de provas e questões relacionadas a competência. Além desses aspectos, também será tratado nesse capítulo as decisões e jurisprudências já existentes no nosso ordenamento jurídico referente ao tema.

3.1 Provas

No Direito Processual Penal as provas são um instrumento de reconstrução aproximada de um fato já ocorrido. Destina-se a formação da convicção do juiz acerca da existência ou inexistência desse fato, sendo assim, busca-se comprovar através das provas a verdade de uma alegação, ou a falsidade de uma afirmação. As provas são de extrema importância pois são um elemento fundamental para uma decisão justa.

Conforme Fernando Capez:

Sem dúvida alguma, o tema referente à prova é o mais importante de toda a ciência processual, já que as provas constituem os olhos do processo, o alicerce sobre o qual se ergue toda a dialética processual. Sem provas idôneas e válidas, de nada adianta desenvolverem-se aprofundados debates doutrinários e variadas vertentes jurisprudenciais sobre temas jurídicos, pois a discussão não terá objeto. (2021, p. 143)

Sendo assim, as provas precisam ser idôneas e válidas para serem acrescentadas no processo, são essenciais e o alicerce que serve de base tanto para a reconstrução do fato histórico, quanto para a construção do convencimento do juiz,

vez que o juiz é, em tese, um desconhecido em relação aos fatos e irá conhecê-lo somente através das provas.

Vale ressaltar que há uma distinção entre meios de prova e meios de obtenção de prova, Aury Lopes Júnior distingue:

a) Meio de prova: é o meio através do qual se oferece ao juiz meios de conhecimento, de formação da história do crime, cujos resultados probatórios podem ser utilizados diretamente na decisão. São exemplos de meios de prova: a prova testemunhal, os documentos, as perícias etc. b) Meio de obtenção de prova: ou *mezzi di ricerca della prova* como denominam os italianos, são instrumentos que permitem obter-se, chegar-se à prova. Não é propriamente “a prova”, senão meios de obtenção. Explica MAGALHÃES GOMES FILHO que os meios de obtenção de provas não são por si fontes de conhecimento, mas servem para adquirir coisas materiais, traços ou declarações dotadas de força probatória, e que também podem ter como destinatários a polícia judiciária. Exemplos: delação premiada, buscas e apreensões, interceptações telefônicas etc. Não são propriamente provas, mas caminhos para chegar-se à prova. (2019, p. 424)

Todos fatos que não são evidentes, notórios, presunções legais ou inúteis, precisam ser provados, inclusive os fatos admitidos pelas partes. Além disso, a prova necessita ser permitida pela lei ou costumes judiciários, fundada, ou seja, ter relação com o processo, um meio para esclarecer questão controvertida e possível de realização, tendo essas características a prova não pode ser denegada. (CAPEZ, 2021)

Além disso, ainda existem as provas proibidas, que não admitidas no ordenamento jurídico nem valoradas no processo, são aquelas contrárias a uma norma legal ou produzida por meios ilícitos. Nesse contexto, a prova será ilícita quando for produzida mediante prática de crime, como por exemplo uma confissão obtida com emprego de tortura, assim como as provas que violem normas de Direito Civil, Comercial, Administrativo e constitucional. E será ilegítima quando afrontar norma legal, por exemplo, o documento exibido em plenário do Júri com desobediência ao artigo 479, do Código de Processo Penal. (CAPEZ, 2021)

As provas proibidas são regulamentadas pelo artigo 157, do Código de Processo Civil dispondo: “São inadmissíveis, devendo ser desentranhadas do processo, as provas ilícitas, assim entendidas as obtidas em violação a normas

constitucionais ou legais”. Da análise do artigo extrai-se que o Código não diferencia ilícita de ilegítima, se referindo a ambas apenas como ilícita. (BRASIL, 1941, *online*)

No ordenamento jurídico brasileiro, não há impedimento para a utilização de provas eletrônicas. Conforme o artigo 225, do Código Civil, podem ser meios de prova fotografias, registros cinematográficos e fonográficos, reprodução eletrônica de fatos, desde que a parte contrária não lhes impugnar. Além disso, o artigo 332, também do Código Civil, abre margem para outros meios não especificados no referido Código, que sejam legais e legítimos, sejam hábeis para servir como prova. (BRASIL, 2002)

Já no Código de Processo Penal, o artigo 231 e 232 também regulamentam acerca das provas e da possibilidade de se utilizar de documentos públicos e particulares em qualquer fase do processo, não fazendo qualquer ressalva sobre os documentos eletrônicos. Ocorre que, a limitação de prova dos crimes virtuais não está nos meios, mas sim na obtenção das provas, pois em muitas das vezes os criminosos agem de forma anônima e que não deixam o mínimo de suspeitas possíveis, eles têm como aliados vasto arcabouço tecnológico que permite agirem silenciosamente e sem vestígios. (BRASIL, 1941)

Em contrapartida, os profissionais responsáveis pela obtenção de provas e competentes para essa função são despreparados, bem como há uma grande deficiência de ferramentas investigativas capazes de desvendar o mundo virtual por trás de tais crimes. Assim, com a carência de aparatos e o despreparo profissional, aumenta-se o grau de dificuldade em identificar os agentes criminosos.

Nesse sentido, expõe Jéssica Olivia, *et al*:

É importante que haja um trabalho de aperfeiçoamento de práticas para o combate dos crimes praticados no ambiente virtual, que sejam; desenvolvimento especializado dos profissionais, capacitação de informática, investimentos em tecnologias que aumente as possibilidades de busca dos delitos, treinamento de policiais, criação de mais delegacias com profissionais voltados para a área virtual e a atualização do legislador em meio à criação de novas condutas, para que se possam criar leis que se adequem a situação. Os crimes só tendem a aumentar, a tecnologia a cada dia avança, esses acontecimentos requerem que as autoridades ajam de igual magnitude. (2018, *online*)

Outra limitação na questão das provas criminais é a necessidade de perícia, em que o perito necessita de uma autorização da autoridade competente para verificar a máquina do suspeito ou a obtenção de informações pelo endereço de IP. Porém, os provedores não armazenam as informações por muito tempo, sendo assim, se a autoridade competente demora a autorizar, a eficácia do trabalho é comprometida.

Desse modo, verifica-se que os avanços que ocorreram em relação aos crimes cibernéticos, são poucos diante do grande mundo virtual e suas nuances, vez que há limitações em várias esferas do direito. Assim como, há muitos casos que não são nem descobertos por falta de denúncia e descrença das vítimas quanto a punição que acarreta esses delitos.

3.2 Competência

Antes de conceituar o que é competência, faz-se necessário uma compreensão acerca do que se trata a jurisdição, pois existe uma distinção entre os dois temas. A jurisdição, em suma, é o poder do Estado em dizer e aplicar a lei, já a competência é a delimitação desse poder, feita através das normas. Nucci preceitua que a jurisdição “é o poder atribuído, constitucionalmente, ao Estado para aplicar a lei ao caso concreto, compondo litígios e resolvendo conflitos.” (2021, p. 156)

Para Manzini, citado por Fernando Capez:

A jurisdição é a função soberana, que tem por escopo estabelecer, por provocação de quem tem o dever ou o interesse respectivo, se, no caso concreto, é aplicável uma determinada norma jurídica; função garantida, mediante a reserva do seu exercício, exclusivamente aos órgãos do Estado, instituídos com as garantias da independência e da imparcialidade (juízes) e da observância de determinadas formas (processo, coação indireta) (2021, *apud*, p. 100)

A jurisdição é una, no entanto apenas um juiz não é capaz de julgar todas as causas do país. Assim, a competência é a medida da jurisdição, através dela é limitado quais órgãos poderá dizer o direito em relação a determinada matéria, localidade ou personalidade. Enfim, todo magistrado possui jurisdição, mas a competência vai depender de normas fixadas através das leis. Fernando Capez conceitua “competência é a delimitação do poder jurisdicional (fixa os limites dentro dos quais o juiz pode prestar jurisdição). Aponta quais os casos que podem ser

julgados pelo órgão do Poder Judiciário. É, portanto, uma verdadeira medida da extensão do poder de julgar. ” (2021, p. 100)

Já Guilherme de Souza Nucci, conceitua competência como:

Trata-se da delimitação da jurisdição, ou seja, o espaço dentro do qual pode determinada autoridade judiciária aplicar o direito aos litígios que lhe forem apresentados, compondo-os. O Supremo Tribunal Federal tem competência para exercer sua jurisdição em todo o Brasil, embora, quanto à matéria, termine circunscrito a determinados assuntos. Não pode, por exemplo, o Ministro homologar uma separação consensual de casal proveniente de qualquer parte do país, embora possa, conforme o caso, apreciar um habeas corpus de pessoa presa em qualquer ponto do território brasileiro. O juiz de uma pequena cidade pode tanto homologar a separação consensual de um casal residente no mesmo local, quanto analisar uma prisão ilegal realizada por autoridade policial da sua Comarca. Não pode, no entanto, julgar casos pertinentes à Comarca vizinha. (2021, p. 157)

Verifica-se, portanto, que quando ocorre um crime virtual deve-se observar, a princípio, em qual território a ação ocorreu. No entanto, na *internet* há uma grande dificuldade em determinar um território, vez que trata-se de um ambiente global em que pessoas de um país pode registrar sites em outros países, assim como, estar em um país realizando uma ação criminosa em outro país.

O ambiente virtual não dispõe de fronteiras territoriais, é um local abstrato, onde não há existência física. O que vigora são normas técnicas que regulam o acesso dos usuários. Assim, os conceitos de soberania e competência territorial perdem sua funcionalidade. No entanto, no que diz respeito a competência para processar e julgar crimes virtuais, na legislação brasileira é aplicado o artigo 5º e 6º do Código Penal, os quais preveem que quando o crime for cometido no território nacional aplica-se a lei brasileira. (BRASIL, 1940)

3.3 Decisões dos tribunais

É sabido que na ausência de um aparato legislativo, cabe aos Tribunais discutir dadas matérias e analisá-las. As jurisprudências apresentam notória relevância no Direito. “Sob tais premissas, embora a jurisprudência seja fonte subsidiária, seu papel é fundamental na produção do Direito. Ainda que não seja obrigatória, sua contribuição é importantíssima para a formação viva do Direito, no preenchimento de lacunas da lei e na sua interpretação. ” (VENOSA, 2019, p. 136)

3.3.1 Crime de calúnia

A *internet* é um ambiente democrático, é um local de debates e uma vitrine onde são expostas diversas formas de pensamentos. Contudo, é importante ter consciência de que as opiniões se tornaram públicas, e caso sejam expressões criminosas devem assumir as respectivas consequências, a exemplo disso são os crimes contra a honra praticados no ambiente virtual.

Para Nucci:

Conceito de honra: é a faculdade de apreciação ou o senso que se faz acerca da autoridade moral de uma pessoa, consistente na sua honestidade, no seu bom comportamento, na sua respeitabilidade no seio social, na sua correção moral; enfim, na sua postura calcada nos bons costumes. Essa apreciação envolve sempre aspectos positivos ou virtudes do ser humano, sendo incompatível com defeitos e más posturas, embora não se trate de um conceito absoluto, ou seja, uma pessoa, por pior conduta que possua em determinado aspecto, pode manter-se honrada em outras facetas da sua vida. Honra não pode ser, pois, um conceito fechado, mas sempre dependente do caso concreto e do ângulo que se está adotando. (2021, p.731)

Nesse sentido, o STJ estabeleceu o entendimento, através do conflito de competência n. 97201 de que no crime de calúnia praticado virtualmente, por meio da *internet*, a competência é firmada pelo local onde se encontra a sede do provedor do site. Nesse sentido vão surgindo jurisprudências que instruem os operadores do Direito em relação ao caminho a se tomar nesses casos. (STJ, 2011)

3.3.2 Imagens vazadas e a Lei geral de proteção de dados

A Lei n. 13.709/2018, dispõe acerca do tratamento de dados pessoais, por pessoas naturais ou jurídicas, objetivando a proteção dos direitos fundamentais de privacidade, liberdade e o livre desenvolvimento da personalidade (BRASIL, 2018). Sendo assim, a Lei geral de proteção de dados está fundamentada nos princípios de liberdade de expressão, privacidade, não violação a intimidade e, também, aos direitos humanos.

A Lei geral de proteção de dados, que entrou em vigor a partir de agosto de 2020, busca a segurança jurídica e a promoção de proteção dos dados pessoais de todo cidadão. Além disso, a lei estabelece que se há o processamento de dados de pessoas que estejam no território nacional, a lei deve ser cumprida, não importando

a localização do centro de dados. Estabelece também, sobre a essencialidade do consentimento, que é a base para o tratamento de dados. (SEPRO, s.d.)

Nesse diapasão, em 2017, o STJ indenizou uma mulher em R\$ 114 mil reais por ter sido vítima de vazamento de imagens íntimas na *internet*. Conforme entendimento do relator, a repercussão na internet aumenta o sofrimento da vítima e causa transtornos imensuráveis, violando seu direito à intimidade. Por fim, frisou que tal conduta envolve diferentes práticas ofensivas criminosas tais como *ciberbullying* e difamação. (CONJUR, 2019)

3.3.3 Comércio online

O comércio *online* vem ganhando mais força com o decorrer dos anos, principalmente com o advento da pandemia da Covid-19 em que as pessoas tiveram que se isolar e a única possibilidade de compra seria através da *internet*. Com isso, as empresas se adaptaram ao ambiente virtual e outras surgiram nesse período. Além de novas empresas, também surgiram novas preocupações com a atuação de quadrilhas criando sites na internet para comercializar produtos sem a intenção de entrega-los.

No entanto, o STJ estabeleceu o entendimento de que:

CONFLITO NEGATIVO DE COMPETÊNCIA. JUÍZES ESTADUAIS DE COMARCAS DE ESTADOS DIFERENTES. INQUÉRITO POLICIAL. ASSOCIAÇÃO CRIMINOSA. CRIAÇÃO DE SITE NA INTERNET PARA COMERCIALIZAR MERCADORIAS QUE JAMAIS SERIAM ENTREGUES: CONDUTA QUE SE AMOLDA MAIS AO CRIME CONTRA A ECONOMIA POPULAR DO QUE AO ESTELIONATO. CONEXÃO TELEOLÓGICA E INSTRUMENTAL ENTRE OS DELITOS. COMPETÊNCIA DEFINIDA PELO LOCAL DA INFRAÇÃO QUE TEM A PENA MAIS GRAVE (ART. 78, II, "A", CPP).
1. A criação de site na internet por quadrilha, sob o falso pretexto de vender mercadorias, mas sem a intenção de entregá-las, amolda-se mais ao crime contra a economia popular, previsto no art. 2º, inciso IX, da Lei n. 1.521/1951, do que ao estelionato (art. 171, caput, CP), dado que a conduta não tem por objetivo enganar vítima(s) determinada(s), mas, sim, um número indeterminado de pessoas, vendendo para qualquer um que acesse o site. [original sem grifos] (BRASIL. Superior Tribunal de Justiça. Conflito de Competência nº 133.534/SP, Rel. Ministro REYNALDO SOARES DA FONSECA, TERCEIRA SEÇÃO, julgado em 28/10/2015, DJe 06/11/2015)

Nesse sentido, a criação de um site com fito de comercializar produtos fictícios pela internet, não atinge apenas uma vítima, mas, na verdade, o objetivo é

atingir toda e qualquer pessoa que acesse ao site, enquadrando-se como um crime contra a economia popular.

3.3.4 *Extorsão pela internet*

Em outro entendimento, o STJ manteve a prisão preventiva de um jovem acusado de praticar crimes sexuais e extorsão contra mulheres pela *internet*. Em suas considerações o relator apontou que o acusado se aproveitou da vulnerabilidade das vítimas no ambiente virtual para praticar extorsão. Destacou ainda, que o anonimato, possibilitado pelo ambiente virtual, impulsionam esses indivíduos a praticarem atos de exploração do corpo feminino. (CONJUR, 2019)

Além dessas jurisprudências, existem outros julgados fixando entendimentos e teses acerca dos crimes praticados virtualmente. A repreensão destes delitos é uma das formas de combate. Embora os crimes aconteçam no ciberespaço, as vítimas são reais e sofrem danos reais, sejam eles patrimoniais ou psicológicos.

Por fim, a prevenção também é um bom remédio. O cuidado na navegação, com sites e e-mails suspeitos, a proteção de dados e mídias, bem como evitar compartilhar certos dados são algumas formas de prevenção. Ademais, em caso de ocorrência de crime virtual, a denúncia é essencial para combater esse e eventuais crimes que poderiam acontecer posteriormente, embora, muitas das vezes despreparada, a polícia é a responsável por conduzir uma investigação mais eficaz.

CONCLUSÃO

A presente pesquisa abordou acerca dos delitos virtuais, do tratamento legal e das limitações no combate aos crimes cibernéticos. Como nos crimes comuns, os crimes virtuais se aperfeiçoam com o tempo abrangendo delitos de roubo de senhas bancárias, chantagens, crimes de conteúdo sexual infantil, ameaças, difamações, e várias outras práticas que aumentam de acordo com o avanço da tecnologia.

O tema disposto é muito relevante e atual e apresenta a realidade dos crimes virtuais na sociedade. Em situações em que ocorrerem e forem comprovados a prática desses delitos, os autores devem ser responsabilizados. Ainda que o ambiente virtual proporcione um sentimento de liberdade, a Constituição Federal de 1988 garante a livre manifestação, mas veda o anonimato que é uma das características principais dos crimes virtuais. Bem como, o Direito de privacidade, protege a vida privada e a intimidade dos indivíduos, sendo uma forte figura jurídica na defesa dos direitos, mesmo em âmbito virtual.

Além disso, é característica do Direito Penal a tutela de bens e direitos. No entanto, um dos princípios básicos do direito penal é o da legalidade, muitos atos ilícitos que têm previsão na legislação penal são praticados por meio do computador, como os crimes de pornografia infantil, calúnia e difamação, fraudes virtuais, estelionato entre outros, esses crimes são punidos independentes se praticados no mundo real ou virtual.

Em contrapartida, surgiram ao longo dos anos, outras legislações, com o fito de tratar e punir os crimes virtuais. Dentre elas, a Lei nº 12.737 de 2012, que tipificou o crime de invasão de dispositivo de informática, e alterou artigos do Código

Penal adequando-os a realidade cibernética. Outra importante legislação para o ambiente virtual, foi o Marco Civil da *Internet*, que surgiu para regulamentar, estabelecer direitos, deveres, princípios e garantias no ciberespaço.

Além da legislação nacional, os crimes virtuais também são resguardados pelo direito penal internacional, vez que a *internet* ocorre em escala mundial. Na ceara internacional, a Convenção de Budapeste sobre o *cibercrime* inovou na forma de cooperação penal e regulamentou formas eficientes de combate aos *cibercrimes*. A convenção abrande fraudes de informática, violações de direito autoral, pornografia infantil e invasões de computadores.

Já na esfera judicial, percebe-se que há uma limitação na obtenção de provas, diante no anonimato proporcionado pela *internet*, bem como uma deficiência de ferramentas investigativas capazes de desvendar o mundo virtual e os autores por trás dos crimes. Além disso, outra limitação observada é a demora na realização de perícia em determinados crimes, o que acaba prejudicando a eficácia do trabalho, vez que os provedores não armazenam informações por muito tempo.

Embora o tema seja atual, já existem diversas decisões de tribunais contribuindo para o preenchimento de lacunas em relação aos crimes virtuais. Exemplo disso, é o entendimento do STJ de que no crime de calúnia praticado virtualmente a competência é firmada pelo local onde se encontra a sede do provedor do site. Tais decisões e jurisprudências instruem os operadores do Direito e possuem notória relevância no ordenamento jurídico.

Por fim, a *internet* e as novas tecnologias influenciam e modificam todas as esferas da vida em sociedade. As redes sociais se tornam cada vez mais poderosas e a privacidade menos valorizada. Com isso, vários dados e informações pessoais correm livremente no mundo virtual, expondo milhares de pessoas e as deixando vulneráveis a prática de crimes. Diante disso, está a importância da conscientização em relação os riscos que a *internet* pode causar. É sempre válido frisar que o usuário deve se proteger de sites duvidosos, bem como utilizar as redes com sabedoria.

REFERÊNCIAS

AKCHAR, Jamili. Breve análise dos princípios essenciais do Marco Civil da Internet – Lei 12.965/14. **Jusbrasil**. 2017. Disponível em: <https://jamili.jusbrasil.com.br/artigos/435150451/breve-analise-dos-principios-essenciais-do-marco-civil-da-internet-lei-12965-4#:~:text=O%20Marco%20Civil%20da%20Internet,da%20rede%2C%20conforme%20a%20seguir>. Acesso em: 18 Feb. 2021.

ALMEIDA, Daniel Freire e. **Um tribunal internacional para a internet**. São Paulo. Almedina. 2015.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 18 Nov. 2020.

BRASIL. **Decreto-Lei nº 3.689, de 03 de outubro de 1941**. Institui o Código de Processo Penal. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 26 maio. 2021.

BRASIL. **Decreto-Lei no 2.848, de 7 de dezembro de 1940** (Código Penal). Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso at: 23 Apr. 2021.

BRASIL. **Lei nº 12735, de 30 de novembro de 2012**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 4 Mar. 2021.

BRASIL. **Lei nº 12737, de 30 de novembro de 2012**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 25 Feb. 2021.

BRASIL. **Lei nº 12965, de 23 de abril de 2014**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 19 Feb. 2021.

BRASIL. **Lei nº 13. 709, de 14 de agosto de 2018**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 26 maio. 2021.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990** . Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Planalto.gov.br. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 12 Nov. 2020.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002.** Institui o Código Civil. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 26 maio. 2021.

BRASIL. **Projeto de Lei nº 4287/2019 - Senado Federal.** Senado.leg.br. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/137947>. Acesso em: 4 Mar. 2021.

BRASIL. Superior Tribunal de Justiça. Conflito de Competência nº 133.534/SP, Rel. Ministro REYNALDO SOARES DA FONSECA, TERCEIRA SEÇÃO, julgado em 28/10/2015, DJe 06/11/2015. **Diário de Justiça Eletrônico.** Disponível em: <https://scon.stj.jus.br/SCON/pesquisar.jsp>. Acesso em: 06 Mai 2021

BRITO, Auriney Uchoa de. O bem jurídico-penal dos delitos informáticos. **Boletim IBCCrim**, n. 199, 2009.. Disponível em: <https://www.ibccrim.org.br/noticias/exibir/4800/>. Acesso em: 26 Feb. 2021.

CAPEZ, Fernando. **Curso de processo penal.** 27. ed. – São Paulo : Saraiva Educação, 2020

CAPEZ, Fernando. **Curso de processo penal.** 28. ed. – São Paulo: Saraiva Educação, 2021.

CARNEIRO, Adeneele Garcia. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. 2012. **Âmbito Jurídico.** Disponível em: <https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-uma-reflexao-sobre-o-problema-na-tipificacao/#:~:text=Na%20d%C3%A9cada%20de%2070%20a,%C3%A0%20necessidade%20de%20se%20despender>. Acesso em: 16 Nov. 2020.

CCJ APROVA PROJETO QUE AGRAVA PENA PARA CRIMES CIBERNÉTICOS – NOTÍCIAS. **CCJ aprova projeto que agrava pena para crimes cibernéticos** - Notícias. Portal da Câmara dos Deputados. Disponível em: <https://www.camara.leg.br/noticias/594044-ccj-aprova-projeto-que-agrava-pena-para-crimes-ciberneticos/>. Acesso em: 4 Mar. 2021.

COLARES, Rodrigo Guimarães. Cybercrimes: os crimes na era da informática. 2002. **Jus.com.br.** Disponível em: <https://jus.com.br/artigos/3271/cybercrimes-os-crimes-na-era-da-informatica#:~:text=Dessa%20forma%2C%20s%C3%A3o%20crimes%20que,obsce no%2C%20escrito%20ou%20objeto%20obsceno%2C>. Acesso em: 23 Nov. 2020.

DELMANTO, Celsom *et al.* **Código Penal comentado.** 9. ed. rev., atual. e ampl. — São Paulo : Saraiva, 2016.

DRUMMOND, Victor. **Internet, privacidade e dados pessoais.** Rio de Janeiro; Lumen Juris, 2003.

G1 > Política - NOTÍCIAS - Brasil é o quarto no ranking da pedofilia, diz PF. **Globo.com.** Disponível em: <http://g1.globo.com/Noticias/Politica/0,,MUL747259->

5601,00-BRASIL+E+O+QUARTO+NO+RANKING+DA+PEDOFILIA+DIZ+PF.html.
Acesso em: 12 Nov. 2020.

GATTO, Victor Henrique Gouveia apud DELMANTO, Celso. **Código Penal Comentado**. 6 ed. atual. e amp. Rio de Janeiro: Renovar, 2002.

GRECO, Rogério. **Curso de Direito Penal: parte especial, volume III**. 11 Ed. Rio de Janeiro: Impetus, 2014.

JESUS, Damásio de; MILAGRE, José Antonio. **Marco civil da internet: comentários à Lei n. 12.965/14**. São Paulo: Saraiva, 2014.

LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional**. Campinas, SP: Ed. Millennium, 2005.

LOPES JÚNIOR, Aury. **Direito processual penal**. 16. ed. – São Paulo : Saraiva Educação, 2019.

LOPES, Jéssica. **Mecanismo de Cooperação Internacional de Repressão e Combate dos crimes cibernéticos**. s.d. Disponível em: <https://egov.ufsc.br/portal/sites/default/files/134-469-1-pb.pdf>. Acesso em 03 Mar. 2021.

MACHADO, Bruna de Oliveira; MATTOS, Karoline Reis; SIQUEIRA, Marcela; *et al.* Crimes Virtuais e a Legislação Brasileira. 2017. **(Re)pensando Direito**. Disponível em: <https://core.ac.uk/download/pdf/229767447.pdf>.

MARCACINI, Augusto Tavares Rosa. **Aspectos Fundamentais do Marco Civil da Internet: Lei nº 12.965/2014**. São Paulo: Edição do autor, 2016.

MEDINA, José Miguel Garcia. **Constituição Federal comentada**. 3. ed. rev., atual. e ampl. – São Paulo: Editora Revista dos Tribunais, 2014.

MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. **Curso de direito constitucional**, 6. Ed. São Paulo: Saraiva, 2011.

NIC.BR. **CGI.br - Comitê Gestor da Internet no Brasil**. CGI.br - Comitê Gestor da Internet no Brasil. Disponível em: <https://cgi.br/portarias/numero/147/>. Acesso em: 12 Nov. 2020.

NIC.BR. **CGI.br - Comitê Gestor da Internet no Brasil**. CGI.br - Comitê Gestor da Internet no Brasil. Disponível em: <https://www.cgi.br/sobre/>. Acesso em: 12 Nov. 2020.

NUCCI, Guilherme de Souza. **Código penal comentado**. 21. ed. – Rio de Janeiro : Forense, 2021

NUCCI, Guilherme de Souza. **Estatuto da criança e do adolescente comentado**. 4a ed. rev., atual. e ampl. – Rio de Janeiro: Forense, 2018.

NUCCI, Guilherme de Souza. **Manual de Processo Penal**. 2. ed. – Rio de Janeiro: Forense, 2021.

OLIVEIRA JÚNIOR, João Batista Caldeira de. A Internet e os “novos” crimes virtuais. 2001. **Jus.com.br**. Disponível em: <https://jus.com.br/artigos/2097/a-internet-e-os-novos-crimes-virtuais>. Acesso em: 12 Nov. 2020.

FROTA, Jéssica Olivia Dias, PAIVA, Maria de Fátima Sampaio. **Crimes Virtuais e a dificuldade para combatê-los**. 2017. Disponível em: https://flucianofejiao.com.br/novo/wp-content/uploads/2018/11/ARTIGO_CRIMES_VIRTUAIS_E_AS_DIFICULDADES_PARA_COMBATE_LOS.pdf. Acesso at: 23 Apr. 2021.

PAESANI, Liliana Minardi. **Direito e Internet : liberdade de informação, privacidade e responsabilidade civil**. – 7. ed. – São Paulo : Atlas, 2014.

Perrone-Moisés, Cláudia. **Direito internacional penal : imunidades e anistias**. Barueri, SP : Manole, 2012.

PINHEIRO, Reginaldo César. Os cybercrimes na esfera jurídica brasileira. 2000. **Jus.com.br**. Disponível em: <https://jus.com.br/artigos/1830/os-cybercrimes-na-esfera-juridica-brasileira>. Acesso em: 11 Nov 2020..

Projeto prevê punição mais rigorosa para crimes virtuais. **Senado Federal**. Disponível em: <https://www12.senado.leg.br/noticias/materias/2020/08/14/projeto-preve-punicao-mais-rigorosa-para-crimes-virtuais#:~:text=O%20Senado%20analisa%20projeto%20de,n%202.848%2C%20de%201940>). Acesso em: 4 Mar. 2021.

ROCHA, Carolina Borges. A evolução criminológica do Direito Penal: Aspectos gerais sobre os crimes cibernéticos e a Lei 12. 737/2012. **Jus Navigandi**. 2013. Disponível em: https://amab.websiteseguro.com/wp/wp-content/uploads/2020/01/A_evolucao_criminologica_do_Direito_Penal.pdf. Acesso em: 25 Feb. 2021

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004.

Saiba como os crimes na internet são tratados em outros países - Notícias. Portal da Câmara dos Deputados. 2011. Disponível em: <https://www.camara.leg.br/noticias/217913-saiba-como-os-crimes-na-internet-sao-tratados-em-outros-paises/>. Acesso em: 4 Mar. 2021.

SALOMÃO, George; Lemos, Ronaldo, *et, al*. **Marco Civil da Internet**. São Paulo: Atlas, 2014.

SERPRO – Serviço Federal de Processamento de dados. O que muda com a LGPD - Lei Geral de Proteção de Dados Pessoais | **Serpro**. 2018. Disponível em: <https://www.serpro.gov.br/lgpd/menu/a-lgpd/o-que-muda-com-a-lgpd>. Acesso at: 25 Mai 2021.

VANIN, Carlos Eduardo. Propriedade Intelectual: conceito, evolução histórica e normativa, e sua importância. **Jusbrasil**. Disponível em: <https://duduhvanin.jusbrasil.com.br/artigos/407435408/propriedade-intelectual-conceito-evolucao-historica-e-normativa-e-sua->

