UNIVERSIDADE TIRADENTES – UNIT

CURSO DE GRADUAÇÃO EM DIREITO

ASSESSORIA DE TCC – TRABALHO DE CONCLUSÃO DE CURSO

CRIMES CIBERNÉTICOS NA ESFERA PENAL: RESPONSABILIDADES E DANOS MORAIS

Bárbara Raquel Vieira dos Santos Felizola

Orientadora: Profª. Mª. Fernanda Oliveira Santos

ARACAJU - SE

2020

CRIMES CIBERNÉTICOS NA ESFERA PENAL: RESPONSABILIDADES E DANOS MORAIS

BÁRBARA RAQUEL VIEIRA DOS SANTOS FELIZOLA

Trabalho de Conclusão de Curso apresentado ao curso de bacharelado em Direito da Universidade Tiradentes, como requisito parcial à obtenção do grau de bacharel em Direito.

Aprovado em _____/_____/_____.

Banca Examinadora

_____

Profª. Mª. Fernanda Oliveira Santos
Professor Orientador
Universidade Tiradentes

_____

Professor Examinador
Universidade Tiradentes

_____

Professor Examinador
Universidade Tiradentes

CRIMES CIBERNÉTICOS NA ESFERA PENAL: RESPONSABILIDADES E DANOS MORAIS

CYBER CRIMES IN THE CRIMINAL SPHERE: RESPONSIBILITIES AND MORAL DAMAGE

Bárbara Raquel Vieira dos Santos Felizola[1]

RESUMO

O presente estudo vem tratar os crimes de origem digital na esfera penal, sendo assim ele objetiva analisar fazer uma análise dos aspectos históricos e da evolução dos crimes cibernéticos e das suas consequências para a sociedade atual. Especificamente, pretende-se apontar as responsabilidades que esse tipo de crime tem mediante o avanço que ele tem tido nos últimos anos; analisar o que diz a legislação brasileira sobre este tipo de crime, os desafios e sua evolução mediante essa nova prática criminosa e verificar os possíveis danos e ameaças que essa prática criminosa trás aos usuários da internet, além das principais dificuldades encontradas pelos operadores do direito no que diz respeito a punir os infratores. A metodologia é de cunho bibliográfico e descritivo, fazendo uso da literatura acerca dos crimes cibernéticos, os danos causados por essa prática criminal e a busca pelos responsáveis pelos crimes. No final, foram observados a falta de provas que possibilitassem definir responsabilidade aos crimes virtuais, o que leva a autora a futuramente, fazer um maior aprofundamento acerca da temática.

Palavras-chave: Crimes Cibernéticos. Código Penal. Danos Morais. Legislação.

ABSTRACT

This study deals with crimes of digital origin in the criminal sphere, so it aims to analyze and analyze the historical aspects and evolution of cyber crimes and their consequences for today's society. Specifically, it is intended to point out the responsibilities that this type of crime has due to the progress it has had in recent years; analyze what Brazilian legislation says about this type of crime, the challenges and their evolution through this new criminal practice and to verify the possible damages and threats that this criminal practice brings to internet users, in addition to the main difficulties encountered by law enforcement officials with regard to punishing violators. The methodology is bibliographic and descriptive, making use of the literature on cyber crimes, the damage caused by this criminal practice and the search for those responsible for the crimes. In the end, there was a lack of evidence that would make it possible to define responsibility for cybercrime, which leads the author to, in the future, do a deeper study on the subject.

Keywords: Cyber crimes. Penal Code. Moral Damages. Legislation.

1 INTRODUÇÃO

[1] Graduanda em Direito pela Universidade Tiradentes – UNIT. E-mail: felizola54@gmail.com

De acordo com Alves (2018), sabe-se que é grande a facilidade com que a internet é utilizada, principalmente no que se refere a transmissão de dados, ainda segundo o autor, essa velocidade na transmissão torna mais fácil aos criminosos, terem acess as informações dos usuários, que em sua maioria ficam acobertados pelo anonimato, isso dificulta bastante tanto a sua identificação pessoal, como também a sua localização.

Mediante esta constatação de vulnerabilidade que acomete muitos usuários e das facilidades com que esses criminosos conseguem cometer esses delitos e saírem impunes em muitos casos, é que este trabalho se justifica, já que traz a necessidade de uma evolução também do direito e da legislação brasileira nessa esfera, já que a velocidade com que a tecnologia é criada é algo impressionante e inexplicável.

É preocupante a velocidade que esse tipo de crime alcança no mundo, e no Brasil não é diferente, de acordo com dados, no último ano, o número de golpes e crimes aplicados via serviços como o WhatsApp aumentaram significativamente, tornando-se a principal ferramenta para hackers no país (UOL, 2018). Com isso, a atual situação do país em relação a esse tipo de crime é algo assustador quando analisado de forma minuciosa, levando em consideração o alto índice de delitos cometidos. Pois, com o aparecimento e popularização da Internet, surgiu o "mundo virtual" (ALVES, 2018).

Sendo assim, este estudo tem como principal objetivo, fazer uma análise dos aspectos históricos e da evolução dos crimes cibernéticos e das suas consequências para a sociedade atual. Especificamente, pretende-se apontar as responsabilidades que esse tipo de crime tem mediante o avanço que ele tem tido nos últimos anos; analisar o que diz a legislação brasileira sobre este tipo de crime, os desafios e sua evolução mediante essa nova prática criminosa e verificar os possíveis danos e ameaças que essa prática criminosa trás aos usuários da internet, além das principais dificuldades encontradas pelos operadores do direito no que diz respeito a punir os infratores.

Como metodologia utilizou-se de pesquisa bibliográfica e descritiva acerca dos crimes cibernéticos, os danos causados por essa prática criminal e a busca pelos responsáveis pelos crimes. Para isso, foi-se utilizado preferencialmente, autores do âmbito jurídico, face a importância destes para o meio acadêmico de direito.

2 CRIMES DIGITAIS: EVOLUÇÃO E CONCEITO

O crescente acesso da população mundial aos sistemas informatizados, notadamente à rede mundial de computadores, permitiu o encurtamento de distâncias por meio da troca de

arquivos e mensagens on-line entre os usuários da internet, o comércio eletrônico, a interação social através de sites de relacionamento, e tantas outras inovações que contribuíram, efetivamente, para a consolidação da globalização e do desenvolvimento geral da sociedade (ARAÚJO, 2009).

Para Caiado; Caiado (2018), esse fato é perceptível nos últimos anos, com a evolução tecnológica, já que ela acontece em uma escala inigualável, não apenas melhorando os padrões de vida mundiais, mas também facilitando a consecução de diversas modalidades criminosas, entre elas a criação de dos crimes digitais.

Corroborando com esse discurso, Araújo (2009), aponta que nesta linha de raciocínio, o desenvolvimento da informática, a despeito dos avanços tecnológicos alcançados, acarretou na construção de terreno fértil para a criação de condutas criminosas inéditas, somadas às já existentes e descritas no Código Penal[2]. Assim, o computador e o software passaram a ser – ao mesmo tempo – alvo e instrumento da delinquência cibernética.

Com a globalização, a disseminação e uso das Tecnologias da Informação e Comunicação – TIC com os recursos eletrônicos, não estão sendo apenas empregados pelas empresas, mas também sendo mais utilizados na prática de diversos crimes, como estelionato, furto mediante fraude e pornografia infanto-juvenil, entre outros (CAIADO; CAIADO, 2018).

Para Souza (2017), isso ocorre porque o meio digital se trata de um ambiente alheio à realidade física, ainda que influenciado por pessoas que nela habitam, há o surgimento de comportamentos e ações até então não previstas, assim como novos tipos de delitos. Esses delitos são em sua maioria cometidos utilizando os computadores, smartphones, tablets, GPS, câmeras digitais, e outros dispositivos eletrônicos. Segundo Caiado; Caiado (2018). surge então um diferente modelo, que é a necessidade de lidar adequadamente com a análise e as investigações que envolvam o uso desses novos recursos tecnológicos utilizados na prática criminosa.

Levando-se em conta o contexto, esperam-se amplos conceitos ou definições acerca dos crimes digitais ou cibernéticos, no entanto o que se observou entre os autores, é diversas denominações.

De acordo com Schmidt (2014), não há um consenso em relação à denominação dos crimes praticados na esfera digital, sendo eles classificados como crimes de computação,

[2] Para que alguém seja punido mediante o CP, ela deve ser responsabilizada penalmente, sendo ainda necessário que a lei descreva, prévia e minuciosamente, todos os elementos do ato considerado ilícito praticado pelo agente. No caso, determinadas condutas criminosas ocorridas mediante a utilização de sistema informatizado, dispositivo de comunicação ou rede de computadores, igualmente devem estar expressamente definidas em lei (MEDEIROS, 2010, p. 3).

delitos de informática, abuso de computador, fraude informática, em fim, são diversos, não abarcando os conceitos em todos os crimes ligados à tecnologia, com isso, faz-se importante atentarmos ao quando se conceituarmos determinado crime, tendo em vista que existem muitas situações complexas no ambiente virtual.

Para Durbano (2019), os crimes cibernéticos, ou cibercrimes são "atividades ilegais praticadas em ambiente virtual que vão além do roubo de informações financeiras". Segundo o autor, os praticantes dos cibercrimes utilizam-se de computadores e internet para atingir os mais variados objetivos, seja por meio de uma rede pública, privada ou doméstica. Schmidt (2014), ainda aponta que, através do conceito analítico finalista de crime, pode se chegar a conclusão de que crimes cibernéticos são todas as condutas típicas, antijurídicas e culpáveis praticadas contra ou com a utilização dos sistemas da informática.

Portanto, mediante o contexto apresentado, vale salientar sobre a importância da segurança no meio digital, já que a evolução da informática é muito rápida, e nem sempre as legislações podem acompanhá-la. Contudo, vale salientar que os crimes digitais não deixam de ser conduta típica, ilícita e punível aos olhos da lei, já que eles são semelhantes a todos os outros tipos de crimes penais já descritos em nosso ordenamento jurídico (ARAÚJO, 2009).

2.1 Tipos de crimes digitais

Para Carvalho (2014), o ambiente virtual é definido como *cyberespaço*[3]. É atualmente nesse espaço que muitos crimes ocorrem, ficando em alguns casos, até impunes. De acordo com Oliveira (2019), a quantidade de crimes digitais no Brasil cresce sem precedentes de acordo com dados de empresas especializadas em segurança na internet. Segundo Carvalho (2014), No Brasil, os ataques a computadores brasileiros quase triplicaram em 2011 em relação ao ano anterior. No ano de 2012 foram 399.515 registros de problemas com vírus, códigos maliciosos ou tentativas de fraude, enquanto em 2010 eram 142.844.

Nos anos seguintes, Machado (2014) apontou que os "Cibercrimes", "Crimes Cibernéticos", "Crimes Digitais", "Crimes Informáticos", "Crimes Eletrônicos", são termos para definir os delitos praticados contra ou por intermédio de, importam nas menções às condutas de acesso não autorizado a sistemas informáticos, ações destrutivas nesses sistemas, a interceptação de comunicações, modificações de dados, infrações a direitos de autor, incitação

[3] "lugar" virtual no qual a conversação ocorre.

ao ódio e descriminação, escárnio religioso, difusão de pornografia infantil, *bullying*, terrorismo, entre outros.

Oliveira (2019) apontou em 2019 através dos dados levantados pela multinacional Psafe, uma lista de pelo menos cinco tipos de crimes digitais, também chamados de crimes cibernéticos, com grande possibilidade de dominar a rede de computadores e celulares do Brasil no corrente ano, são eles:

- O roubo de dados pessoais;
- O avanço no uso de robôs com inteligência artificial;
- O fim das senhas e o uso cada vez mais frequente de sistemas de dupla identificação;
- O sextorção;
- A sofisticação de golpes.

Ainda segundo Oliveira (2019), os especialistas do laboratório brasileiro da empresa de antivírus Psafe, que monitora a internet em tempo real e registraram 387.424 links maliciosos detectados apenas em um único dia.

2.2 Os desafios na investigação criminal: responsabilidade e danos dos crimes digitais

O número de crimes praticados no ambiente digital é sem precedentes, fato apontado por Araújo (2009), quando ele destaca o quanto esta forma de delinquência é maior do que se imagina, já que a capacidade de o computador e o software virem a ser, igualmente, objeto ou instrumento da conduta proibida.

No Brasil, isso é notório já que a rede é acessada por pessoas de todas as faixas etárias, não havendo muito controle sobre o contato entre elas em salas de bate-papo ou canais de venda, ou mesmo o acesso a conteúdos violentos e/ou pornográficos (DULLIUS; HIPPLER; LUNARDI, 2012).

Na legislação brasileira estão ocorrendo modificações[4] em alguns textos legais para que estes possam ser adaptados a determinados delitos que crescem impunes, já que se vale de

[4] A Lei n.º 9.983, de 14 de julho de 2000, também trouxe diversas modificações no direito material penal, tendo, como principais mudanças:
a) Criação no art. 153, § 1º-A do Decreto-Lei n.º 2.848/40, do tipo penal de divulgação de segredo institucional, considerando crime a conduta de "divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública";
b) Criação no art. 313-A do Decreto-Lei n.º 2.848/40, do tipo penal de inserção de dados falsos em sistema de informações, que considera crime a conduta de "inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano";
e,

recursos oferecidos pela rede mundial de computadores como proxys[5] de anonimato, no entanto, há "muitas condutas reprováveis no plano social e praticadas por meio do uso das tecnologias ainda carecem de uma definição jurídica quanto ao que realmente representam" (CARVALHO, 2014; SCHMIDT, 2014).

Para Schmidt (2014), em relação à materialidade dos crimes digitais de modo geral, pode-se dizer que:

> As evidências dos crimes cibernéticos são extremamente voláteis. Podem ser apagadas em segundos ou perdidas facilmente. Além disso, possuem formato complexo e costumam estar misturadas a uma grande quantidade de dados legítimos, demandando uma análise apurada pelos técnicos e peritos que participam da persecução penal (SCHMIDT, 2014, p. 15).

Além das dificuldades encontradas e impostas pelos servidores de anonimato, e que dificultam bastante às evidências, existe também a questão do sigilo das comunicações, que segundo Covolan e Mesquita (2019, p. 2), é um dos direitos fundamentais descritos no artigo 5º da Constituição Federal de 1988[6]. Entretanto, os autores apontam que "esse direito de sigilo não é absoluto", já que existem exceções para sua preservação, podendo ele ser "quebrado quando houver determinação judicial para tal, como em casos de crimes em que ocorre uma troca de informações entre os envolvidos". Sendo assim, essas exceções garantem não apenas a quebra do sigilo, mas podem também ser utilizados como prova para o julgamento.

Segundo Corrêa (2010), isso ocorre porque algumas empresas que prestam serviços na Internet somente divulgam os dados de conexão com decisão judicial. De acordo com o autor, essas empresas segundo Corrêa (2010, p. 2), "costumam criar embaraços para informar à Autoridade Policial as informações que são necessárias à investigação de crimes que tenham sido cometidos em seus serviços".

Essas atitudes além de atrapalharem as investigações resultam também em prejuízos aos cofres públicos. De acordo com o site de notícias UOL (2018), um relatório da Norton Cyber Security foi divulgado em 2017, nele o Brasil passou a ser o segundo país com maior

---

c) Criação no art. 313-B do Decreto-Lei n.º 2.848/40, do tipo penal de modificação ou alteração não autorizada de sistema de informações, considerando crime a conduta de "modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente".

[5] Servidor intermediário, que atende a requisições repassando os dados do cliente à frente, a outro servidor, que oferece o serviço. Muitas vezes, é utilizada uma cadeia de proxys, tornando a identificação da máquina de origem das ações virtualmente irrastreável.

[6] **Artigo 5º, inciso XII da Constituição:**
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; (BRASIL, 1988).

número de casos de crimes cibernéticos, afetando cerca de 62 milhões de pessoas e causando um prejuízo de US$ 22 bilhões. Portanto, o que se nota é que "apesar de tímidas as iniciativas legislativas, já temos um pequeno rol de aparato normativo para auxiliar o Estado no combate a determinadas condutas delitivas" (CARVALHO, 2014, p. 1).

2.4 A legislação brasileira

De acordo com Medeiros (2010), o Código Penal Brasileiro – CPB hoje em bastante aceitação teve várias atualizações, o que é de extrema importância, já que sua estrutura e redação original são de 1940, ou seja, mais velha que a nossa Constituição Federal e tendo sido criada cinco décadas antes da Revolução Digital.

Isso mostra o quanto a sociedade mudou muito desde então, e em ritmo cada vez mais acelerado desde a década de 1980, com o crescimento cada vez maior das TICs, o que nos leva a pensar que a legislação brasileira deve seguir nesse ritmo, para que assim possa acompanhar essa evolução, já que o digital avança de forma acelerada como aponta Laflouva (2011):

> O problema do mundo digital, é que ele não tem fronteiras, enquanto que a legislação é aplicada de acordo com a localidade de realização do suposto crime cibernético. Sabendo disso, hackers de todo o mundo têm aprendido a burlar as leis, hospedando seus sites em países de legislação mais flexível, como a Eslovênia ou a Suíça, e usando artimanhas digitais para que seus acessos via IP apontem para regiões onde a punição judicial a cibercrimes seja mais difícil, com o uso de roxys, sites da web que permitem a navegação de forma supostamente anônima, ao trocar o IP que identifica o computador que realiza determinado acesso (LAFLOUVA, 2011, s/p).

Segundo Carvalho (2014), no Brasil existem modificações em textos legais buscando adaptá-los a legislação a determinados delitos que se valem de recursos oferecidos pela rede mundial de computadores. Contudo, "muitas condutas reprováveis no plano social e praticadas por meio do uso das tecnologias ainda carecem de uma definição jurídica quanto ao que realmente representam" (2014, p. 2).

2.4.1 Marco Civil da internet

A internet por muito tempo foi considerada terra sem lei, nela as fronteiras dos crimes eram sempre escancaradas, ou seja, muitas vezes, um crime na rede tem um autor em um país, e uma vítima em outro, o que dificultava a apuração, já que cada país possui sua própria legislação. No entanto, a partir de abril de 2012 os crimes que eram praticados na rede

passaram a responder a Lei nº 12.965, sancionado em 23 de abril de 2014, sob o desígnio de regulamentar o uso da internet no Brasil, sendo estabelecido garantias, princípios, deveres e direitos (SEGURADO; LIMA; AMENI, 2014; BORTOT, 2017; SOUZA, 2017; OTOBONI; ALMEIDA; CAMPANHOLO, 2019).

A lei surgiu não por conta dos diversos crimes que já ocorriam em meio digital, mas por conta da pressão midiática e pelo clamor de "justiça" da atriz Carolina Dieckmann que teve a fotos intimas vazadas na internet. Na época os infratores que divulgaram as fotos foram localizados e indiciados por extorsão qualificada, furto e difamação (CRUZ; RODRIGUES, 2018).

Segundo Otoboni; Almeida; Campanholo (2019), Marco Civil da Internet (MCI) é considerado como a "constituição da internet". Seu texto é composto por 32 artigos em 5 capítulos. Ele possui cinco principais pontos, por exemplo, direitos, neutralidade, armazenamento de informações, responsabilidade e obrigações do poder público.

Os princípios do Marco Civil da Internet estão especificados nos incisos do Art. 3º da sua lei, a disciplina do uso da internet no Brasil tem os seguintes princípios:

> I – Garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II – Proteção da privacidade;
> III – Proteção dos dados pessoais, na forma da lei;
> IV – Preservação e garantia da neutralidade de rede;
> V – Preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
> VI – Responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
> VII – preservação da natureza participativa da rede;
> VIII – liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei (BRASIL, 2014, p. 1).

No MCI é estabelecida a confidencialidade e a isenção do provedor, porém determina que ele deve fornecer os registros quando judicialmente solicitados:

> Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.
> Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:
> I - fundados indícios da ocorrência do ilícito;
> II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e
> III - período ao qual se referem os registros.
> Art. 23. Cabe ao juiz tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e

> da imagem do usuário, podendo determinar segredo de justiça, inclusive quanto aos pedidos de guarda de registro (BRASIL, 2014, p. 6).

De acordo com Marcacini (2016), a Lei encontrou e regulou alguns fatos sociais que são fruto exclusivo da Internet – como é o caso das disposições que estabelecem a neutralidade da rede ou a responsabilidade dos provedores[7] de Internet, mas resvalou também, e pretendeu regular, situações jurídicas que não são uma exclusividade do ciberespaço:

> A privacidade, a proteção a dados pessoais ou a liberdade de expressão – embora essas possam encontrar na rede uma larga amplitude de casos concretos e, consequentemente, obter maior visibilidade midiática quando ligadas a fatos ocorridos online. Mas é difícil restringir tais situações apenas ao universo da Internet, no que o Marco Civil deixa uma sensação de incompletude, ou de um encaixe imperfeito, no trato dessas matérias (MARCACINI, 2016, p. 31).

Para Otoboni; Almeida; Campanholo (2019), o exposto do MCI demostram que o principal objetivo do princípio da neutralidade é garantir a isonomia dos dados dispostos para os usuários, possibilitando a mesma velocidade do tráfego na rede, buscando o livre acesso de conteúdo depositado nos mesmos dispositivos, com a mesma intensidade da informação para ambas as pessoas que acessem aquilo que foi compartilhado e publicado na internet.

2.6 Os crimes digitais na esfera penal e as jurisprudências

Segundo Araújo (2009), os crimes cibernéticos, aos olhos da lei criminal, não são impunes, mesmo com a capacidade e alcance dos computadores e seus componentes como instrumentos da conduta proibida. Porém de acordo com Medeiros, mesmo com a evolução da legislação, ainda há diversos desafios em uma investigação a crimes ocorridos no meio cibernético.

---

[7] Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.
§ 1o Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no caput a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado.
§ 2o A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no caput, observado o disposto nos §§ 3o e 4o do art. 13.
§ 3o Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.
§ 4o Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência (BRASIL, 2014, p. 5).

Para Bortot (2017), seja qual for a forma de cometimento do crime cibernético, cabe ressaltar que a rapidez da vítima na busca pela atuação judicial ou administrativa competente, é providência que se impõe, na medida em que o desaparecimento dos vestígios da conduta delitiva, ou mesmo do próprio infrator, impossibilitando a apuração de responsabilidades, mostra-se como uma das características principais desta forma de infração à lei penal. O que é comprovado no Art. 154-A do Código Penal, que estabelece:

> 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.
> 1 Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> 2 Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> 3 Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> 4 Na hipótese do § 3 , aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas.
> 5 Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I – Presidente da República, governadores e prefeitos;
> II – Presidente do Supremo Tribunal Federal;
> III – Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV – Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Neste contexto, do bem jurídico tutelado da Lei 12.737/2012, estando previstos no Art. 5º, X da Constituição Federal Brasileira, onde diz que é a inviolabilidades dos dados informáticos, derivado do direito a privacidade e intimidade. Sendo assim, Otoboni; Almeida; Campanholo (2019) afirmam que no Brasil possui legislação material e processual suficientes para a instauração de procedimentos investigatórios e punitivos dos crimes praticados contra e por meio da informática. A atuação estatal depende, portanto, da celeridade de comunicação do ato lesivo e da escolha dos meios adequados, por parte das autoridades competentes, à apuração do delito.

2.6.1 Crimes contra a honra

Para muitos, honra é o que se tem de mais valioso, sendo assim, manchar a honra de alguém não é visto com bons olhos, contudo, no mundo digital, tal prática tornou-se algo comum, já que muitos se sentem protegidos diante das telas de computadores e tabletes, no entanto, hoje temos leis para alguns crimes virtuais[8], elas estão expressas no Código Penal Brasileiro (PRADO, 2008; BERNAL, 2019). Sobre os crimes contra a honra, Prado (2008) os descreve de forma subjetiva e objetiva:

> A honra, do ponto de vista objetivo, seria a reputação que o indivíduo desfruta em determinado meio social, a estima que lhe é conferida; subjetivamente, a honra seria o sentimento da própria dignidade ou decoro. A calúnia e a difamação atingiriam a honra no sentido objetivo (reputação, estima social, bom nome); já a injúria ofenderia a honra subjetiva (dignidade, decoro) (PRADO, 2008, p. 213).

Bernal (2019) descreve cada um dos crimes tipificados como contra a honra e sua previsão no Código Penal Brasileiro:

> **Calúnia:** Falsa imputação de fato criminoso a outro alguém, atingindo a honra da vítima. Todos podem praticar o crime de calúnia, sendo punível também o crime contra os mortos. A acusação caluniosa pode ser feita na ausência do ofendido, mas precisa se divulgar, espalhar, tornar público, devendo haver a intenção de divulgar fato criminoso sabendo ser falso. Previsto no artigo 138 do Código Penal
> **Difamação:** Imputação a alguém de fato ofensivo à sua reputação, atingindo a honra da vítima. Ao contrário da calúnia, não é necessário que a imputação seja falsa, basta a existência do fato desonroso. Previsto no artigo 139 do Código Penal.
> **Injúria:** Ato de atribuir a alguém qualidade negativa que tanto pode ser falsa quanto verdadeira. Não há imputação de um fato, mas sim uma opinião negativa que o agente dá a respeito da vítima. Ela diz respeito à honra subjetiva da pessoa, é o ato de xingamento. A injúria poderá ser cometida na forma verbal, escrita ou mesmo física. Esse ato é considerado crime e está previsto no Código Penal artigo 140.
> **Estelionato digital:** Crime com o objetivo de enganar as vítimas, geralmente, o golpe se inicia com a criação de uma página falsa com utilização de uma identidade visual de empresa para oferecer suposto benefício para as vítimas, com envio de post em redes sociais, links patrocinados. Os criminosos enchem as vítimas de elogios e dão respostas rápidas e atenção. Após extraírem algum dinheiro das vítimas, resta a frustração, pois o fraudador nessa altura já está incomunicável, quando então a vítima percebe que caiu em um golpe. Esse tipo de crime há previsão no Código Penal Brasileiro no artigo 171. (BERNAL, 2019, p. 1-2).

Para ficar mais nítido segue abaixo a jurisprudência de um caso julgado sobre crimes virtuais, no caso abaixo, estelionato:

> 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

[8] Nomeados crimes de calúnia, difamação e injúria, crimes contra a honra, previstos no capítulo V desse diploma legal, em que a sua prática imputa punição ao seu infrator (BERNAL, 2019).

> 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. 2. Nos termos do art. 2º, IX, da Lei n. 1.521/1951, constitui crime contra a economia popular "obter ou tentar obter ganhos ilícitos em detrimento do povo ou de número indeterminado de pessoas mediante especulações ou processos fraudulentos ("bola de neve', 'cadeias', 'pichardismo' e quaisquer outros equivalentes)". 3. Verificada estreita conexão teleológica (art. 76, II, CPP) e probatória (art. 76, III, CPP) entre a associação criminosa e o crime contra a economia popular, no caso concreto, a definição da competência segue a regra posta no art. 78, II, "a", do CPP (local d infração à qual foi cominada a pena mais grave). 4. Dado que o crime de associação criminosa possui pena mais grave (reclusão de 1 a 3 anos) do que a atribuída ao crime contra a economia popular (detenção de 6 meses a 2 anos e multa) e a associação criminosa consumou-se em Goiânia, pois seis dos sete investigados residiam naquela cidade, é forçoso reconhecer a competência do Juízo estadual de Goiânia para conduzir o inquérito policial. 5. Conflito conhecido, para declarar a competência do Juízo de Direito da 8ª Vara Criminal de Goiânia/GO, o suscitado.

O estelionato descrito acima se deu pelo criminoso criar sites na internet para vender mercadorias com a intenção de nunca entregá-las, sendo esta, considerada uma conduta que se amolda ao crime contra a economia popular, previsto no artigo 2º, inciso IX, da Lei 1.521/51, como definiu a corte.

2.6.2 Crimes contra o patrimônio

Segundo Netto Filho (2012), os crimes contra o patrimônio é um problema atual e que deve ser vista com cuidado por nossos legisladores, a omissão legal é algo temeroso, pois ainda que aleguem que nosso Código Penal de 1940 possui feição vanguardista, *concessa vênia*, há uma diferença ainda que tênue entre os crimes praticados no ambiente virtual dos praticados no ambiente real.

Para Redler (2019), os crimes contra o patrimônio estão previstos no Título II do Código Penal, para a autora, é crime contra o patrimônio toda ação que atente contra bens de uma pessoa ou organização, ou seja, o objeto do crime é qualquer coisa que tenha valor patrimonial.

São crimes contra o patrimônio:

- Furto (artigo 155 do CP);
- Roubo (Artigo 157 do CP);
- Extorsão (Artigo 158 do CP);

- Extorsão mediante sequestro (artigo 159 do CP);
- Apropriação indébita (Artigo 168 do CP);
- Estelionato (artigo 171 do CP);
- Receptação (artigo 180 do CP).

Apesar da esfera digital, esses crimes supracitados são comuns, mesmo que em muitos casos os criminosos não estejam no mesmo local que a vítima como é perceptível na jurisprudência abaixo;

> HABEAS CORPUS. FURTO SIMPLES. TENTATIVA. APROXIMADAMENTE R$ 90,00 (DOIS CHUVEIROS). APROXIMADAMENTE 9 % DO SALÁRIO MÍNIMO VIGENTE. VALOR INEXPRESSIVO DA RES FURTIVA. REINCIDÊNCIA EM CRIMES CONTRA O PATRIMÔNIO - ROUBO E FURTO. HABITUALIDADE DELITIVA. PRINCÍPIO DA INSIGNIFICÂNCIA. INAPLICABILIDADE. ORDEM DENEGADA. 1. Embora seja inexpressivo o valor da res furtiva - aproximadamente R$ 90,00 (dois chuveiros) -, correspondente a aproximadamente a 9% do salário mínimo vigente à época, a reincidência em crimes contra o patrimônio - roubo e furto -, além da existência de outras ações penais e inquéritos policiais em curso, são suficientes para afastar a aplicação do princípio da insignificância. Precedentes. 2. Habeas corpus denegado.
> (STJ - HC: 540456 SP 2019/0313276-6, Relator: Ministro NEFI CORDEIRO, Data de Julgamento: 03/12/2019, T6 - SEXTA TURMA, Data de Publicação: DJe 09/12/2019)

Mediante o exposto e cumulando-se ao artigo *suso* mencionado temos o art. 6º do CP, versando sobre o lugar do crime, *vide*: "Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado". Assim, o bem jurídico tutelado é o patrimônio, cuja inviolabilidade se busca garantir com a incriminação (NETTO FILHO, 2012; REDLER, 2019).

2.6.3 Crimes contra a dignidade sexual

Dentre os crimes digitais, os contra a dignidade sexual é um dos mais graves, além de comuns, antigamente eles eram denominados crimes contra os costumes, porém hoje segundo Greco (2011), o Título VI do Código Penal, com a nova redação dada pela Lei no 12.015, de 7 de agosto de 2009, passou a prever os chamados crimes contra a dignidade sexual, modificando, assim, a redação anterior constante do referido Título.

Outra lei que sofreu alteração foi a de Lei 8.069/90 (Estatuto da Criança e do Adolescente), que foi alterada pela Lei 13.441, de 08 de maio de 2017, que prevê a infiltração de agentes de polícia na internet, visando a investigação de crimes contra a dignidade sexual de crianças e adolescentes (TORTORIELLO, 2019).

Segundo Mello (2019), em 2018, foi publicada a lei 13.718/2018, de vigência imediata, a qual alterou significativamente os crimes contra a dignidade sexual e a Lei de Contravenção Penal (Decreto-Lei 3588/41).

Os crimes contra a dignidade sexual são bastante comuns e recorrentes na atualidade, principalmente na esfera digital. Essa prática criminal é das mais infames da sociedade moderna, já que ela abrange principalmente a pornografia infanto-juvenil, e facilitando também o acesso a ele e a distribuição de material a este relacionado. (CAIADO; CAIADO, 2018).

No entanto, com a alteração na legislação, o que ampliou os crimes de natureza sexual, alterando também as penalizações para crimes dessa natureza, no que cerne as decisões judiciais:

> HABEAS CORPUS SUBSTITUTIVO DE RECURSO PRÓPRIO. INADEQUAÇÃO DA VIA ELEITA. CRIME CONTRA A DIGNIDADE SEXUAL. ESTUPRO DE VULNERÁVEL. PORNOGRAFIA INFANTIL. PROVA ILÍCITA. INEXISTÊNCIA. AUTORIA E MATERIALIDADE DEVIDAMENTE COMPROVADAS. NECESSIDADE DE REEXAME DE FATOS E PROVAS HABEAS CORPUS NÃO CONHECIDO. 1. O Supremo Tribunal Federal, por sua Primeira Turma, e a Terceira Seção deste Superior Tribunal de Justiça, diante da utilização crescente e sucessiva do habeas corpus, passaram a restringir a sua admissibilidade quando o ato ilegal for passível de impugnação pela via recursal própria, sem olvidar a possibilidade de concessão da ordem, de ofício, nos casos de flagrante ilegalidade. 2. Neste caso, a defesa alega que a prova que dá suporte à condenação teria sido obtida de modo ilícito, pois decorreu de acesso a dispositivos de armazenamento de dados pertencentes ao paciente sem a devida autorização. Ocorre que os dados foram obtidos pelo seu companheiro durante período em que ambos partilhavam a residência e os bens que guarneciam o imóvel, não se podendo, assim, falar que o acesso foi realizado de maneira clandestina. 3. O acolhimento da tese defensiva depende da desconstituição das conclusões das instâncias antecedentes acerca da propriedade partilhada dos bens entre o paciente e a testemunha. Tal providência, contudo, não é comportada pelos estreitos limites do habeas corpus, em cujo escopo não se admite dilação probatória. 4. Ademais, o conjunto de provas carreado aos autos, dentre as quais estão a confissão do acusado e o depoimento da vítima, são suficientes para manter a sentença condenatória, não havendo que se falar em constrangimento a ser sanado, de ofício, pela via mandamental. 5. Habeas corpus não conhecido.
> (STJ - HC: 531627 SP 2019/0266087-0, Relator: Ministro REYNALDO SOARES DA FONSECA, Data de Julgamento: 21/11/2019, T5 - QUINTA TURMA, Data de Publicação: DJe 09/12/2019)

Portanto, as alterações nas referidas lei amplia a proteção em relação às mulheres, crianças e adolescentes, além de pessoas com deficiência, tipificando o crime de “Importunação Sexual”, divulgação de fotos e vídeos contendo cena de sexo sem o consentimento, aumentando as penas para os crimes de estupro coletivo, além de alterar a natureza da ação penal nos crimes contra a dignidade sexual (MELLO, 2019).

3 O COMBATE E PREVENÇÃO DOS CRIMES VIRTUAIS

Para evitar e combater os crimes cibernéticos, seja na vida pessoal ou profissional, é preciso ser extremamente cuidadoso. Neste sentido, segue algumas dicas para conscientização digital, já que elas são baratas e seguras para o bom uso das tecnologias.

- Use uma suíte de segurança para a internet, para garantir proteção contra vírus e ameaças emergentes da web;
- Use senhas fortes, sem repeti-las em sites diferentes e mude-as regularmente;
- Mantenha todo software atualizado, principalmente sistemas operacionais e suítes de segurança na internet. Os hackers utilizam explorações conhecidas no software para obter acesso ao seu sistema;
- Gerencie as suas configurações de mídias sociais para manter a maior parte das suas informações pessoais e privadas bloqueadas;
- Proteja sua rede doméstica com uma senha de criptografia forte e com uma VPN que irá criptografar todo o tráfego que sai dos dispositivos, até que chegue ao destino desejado;
- Mantenha-se atualizado sobre as grandes violações de segurança.

Com esses cuidados, fica mais difícil de cair nos crimes de rede, no entanto, caso ainda caia neste tipo de crime, faz-se importante buscar os órgãos competentes, como delegacias especializadas neste tipo de crime, já somente a justiça é capaz de julgar e definir quais serão as perdas em consequência destes crimes.

De acordo com a determinação da Constituição Federal de 1988: "XXXIX - não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal". Em relação aos crimes digitais também, já que eles são punidos da mesma forma que se pune qualquer outro crime, tal dispositivo, portanto, determina reserva legal para a tipificação, algo adotado pelo sistema jurídico romano-germânico, também conhecido como *civil law*[9], ao qual o Brasil adere. Portanto, para haver constatação de delito em diversas atividades virtuais, é de suma importância que as provas sejam devidamente preservadas, já que por ser em ambiente virtual, possam ocorrer "imprevistos" (BRASIL, 1988; CAETANO, 2015).

Segundo Caetano (2015), para coletar e preservar as evidências em meio eletrônico deve-se imprimir, salvar arquivos em meio eletrônico, e-mails, prints de telas, ou mesmo a impressão da página pelo escrivão policial (visto que seus atos possuem fé pública), de tudo

[9] Estrutura jurídica onde a aplicação do direito se dá a partir da interpretação da lei. Caso em que a própria lei será usada para justificar a decisão judicial do caso concreto (ROCHA, 2018).

que possa servir como evidencia e possa desaparecer de maneira rápida e sem deixar vestígios. E sempre se lembrar de que todas as provas são importantes para a investigação.

Para Netto Filho (2012), em relação a prevenção e combate aos crimes virtuais, faz-se necessário um diálogo entre sociedade e Governo, no tocante ao interesse na repressão dos crimes virtuais, como também na preservação de direitos já positivados em nosso ordenamento, como por exemplo, a liberdade de expressão, prevalecendo nossos princípios da democracia e do Estado Democrático de Direito.

Para ajudar no combate aos crimes virtuais, temos as Leis como o Marco Civil da Internet (Lei nº 12.965/14) e a Lei Carolina Dieckmann (Lei nº 12.737/12), são elas que auxiliam no combate a esses crimes, mas como já visto, não são suficientes, são leis com penas brandas, e é preciso que a sociedade clame por mudanças, por penalidades mais severas, leis rigorosas, legislação específica e que a sociedade também conheça os crimes e aprendam a lidar com tais situações as quais estamos todos sujeitos.

4 CONSIDERAÇÕES FINAIS

Com base no que foi exposto durante a pesquisa com base nos conceitos para o desenvolvimento deste artigo, pode-se afirmar que os objetivos apresentados na introdução foram em parte alcançados, já que nele vêm elencados alguns dos problemas apontados que justificaram a escolha deste tema. Contudo, ficou difícil definir no estudo apresentado, um responsável por esse tipo de crime, já que nos crimes cibernéticos abrangem um espaço difícil de mensurar, como também são cometidos em locais distintos e de difícil localização pelas autoridades, o que é comum nos crimes de rede.

No entanto, não há como negar os esforços que o poder judiciário vem tendo no combate aos crimes de natureza digital, punindo os infratores com base na legislação vigente, alterando leis antiquadas e buscando atualizar as definições de alguns delitos, tendo alguns, suas definições ampliadas, adaptadas e modificadas, para que assim, possam acompanhar a evolução digital. Já que os crimes digitais são resultantes do processo evolutivo e despreparado da internet, pois, à medida que avançava os métodos de propagação e transferência de dados pela rede, esquecia-se de atribuir um método protetivo voltado à segurança dos usuários.

Conclui-se que o combate aos crimes da informática se faz necessário nos levando a refletir sobre quais seriam os meios de contingência que poderiam levar a sociedade a maior segurança, além disso, trás a necessidade de futuramente fazer um estudo mais aprofundado acerca da temática.

REFERÊNCIAS

ALVES, Maria Hiomara dos Santos. **A evolução dos crimes cibernéticos e o acompanhamento das leis específicas no Brasil**. Disponível em: https://jus.com.br/imprimir/64854/a-evolucao-dos-crimes-ciberneticos-e-o-acompanhamento-das-leis-especificas-no-brasil. Acesso em 21 fev, 2020.

BERNAL, Ana. **Crimes contra a honra na internet** - Direito e Justiça, Jornal Estado de Minas. 2019

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

BRASIL. **Decreto-Lei nº 2.848 de 1940**. Disponível em: http://www.planalto.gov.br/ccivil_03/decretolei/del2848compilado.htm. Consultado em 18 mar. 2020.

BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 2. **Crimes cibernéticos**. 2ª Câmara de Coordenação e Revisão, Criminal. – Brasília: MPF, 2018. 275 p. – (Coletânea de artigos; v. 3) Disponível também em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes.

BRASIL. Presidência da República. **Lei nº 12.965, de 23 de abril de 2014.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 4 fev. 2020.

CAETANO, Aldo Maxwell Pereira de Mesquita. **Crimes virtuais:** aplicação, falibilidade e impunidade. 2015. Disponível em: http://openrit.grupotiradentes.com:8080/xmlui/handle/set/1195. Acesso em 28 mar. 2020.

CAMPELO, Larissa; PIRES, Pamela de Freitas. **Crimes virtuais**. Jus Navigandi, 2017. Disponível em: https://jus.com.br/artigos/72619/crimes-virtuais. Acesso em 25 de maio de 2020.

CARVALHO, Paulo Roberto de Lima. **Crimes cibernéticos:** uma nova roupagem para a criminalidade. 2014. Disponível em: https://jus.com.br/artigos/31282/crimes-ciberneticos-uma-novaroupagem-paraacriminalidade. Acesso em 8 fev. 2020.

COSTA, Daniel. **Direito digital nas esferas criminal e cível**: crimes cibernéticos, responsabilidades e danos morais. Disponível em: https://juridicocerto.com/p/danielcostaadv/artigos/direito-digital-nas-esferas-criminal-e-civel-crimes-ciberneticos-responsabilidades-e-danos-morais-1793. Acesso em 25 maio 2020.

DE LUCCA, Newton; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de; MACIEL, Renata Mota. **Direito e internet IV:** sistema de proteção de dados pessoais. [S.l: s.n.], 2019.

DULLIUS, Aladio Anastacio; HIPLLER, Aldair; FRANCO, Elisa Lunardi**. Dos Crimes Praticados em Ambientes Virtuais.** 2012. Disponível em: http://www.egov.ufsc.br/portal/conteudo/dos-crimes-praticados-emambientes-virtuais. Acesso em 3 fev. 2020.

GRECO, Daniela. **Direito digital:** um dossiê da área e as novas jurisprudências! 2011. Disponível em: https://blog.saraivaaprova.com.br/direito-digital/amp/. Acesso em 25 de maio de 2020.

LAFLOUFA, Jacqueline. **Hackativismo:** crime cibernético ou legítima manifestação digital? 2011. Disponível em: http://comciencia.scielo.br/scielo.php?script=sci_arttext&pid=S1519-76542011000700006&lng=pt. Acesso em 4 fev. 2020.

LIMA, Simão Prado. **Crimes virtuais:** uma análise da eficácia da legislação brasileira e o desafio do direito penal na atualidade. 2014. Disponível em: https://ambitojuridico.com.br/cadernos/direito-penal/crimes-virtuais-uma-analise-da-eficacia-da-legislacao-brasileira-e-o-desafio-do-direito-penal-na-atualidade/. Acesso em 25 de maio de 2020.

MAFRA, Melina. **Crimes cibernéticos:** os desafios no processo investigatório frente à ausência de legislação específica no ordenamento brasileiro. 2013. Disponível em: https://www.webartigos.com/artigos/crimes-ciberneticos-os-desafios-no-processo-investigatorio-frente-a-ausencia-de-legislacao-especifica-no-ordenamento-brasileiro/105048. Acesso em 2 fev. 2020.

MALHEIRO, Emerson Penha. **Delitos virtuais praticados na sociedade da informação**. 2017. Disponível em: http://www.rkladvocacia.com/delitos-virtuais-praticados-na-sociedade-da-informacao/. Acesso em 2 fev. 2020.

MEDEIROS, Claudia Lucio de. **Deficiências da legislação penal brasileira frente aos crimes cibernéticos.** 2010. Disponível em: http://www.mpce.mp.br/esmp/publicacoes/edf_2010/artigos/art05ClaudiaMedeiros.pdf. Acesso em 2 fev. 2020.

MURARD, Ana Beatriz Conte. **Crimes contra a honra na Internet**. Jusbrasil. 2015. Disponível em: https://anabmurard.jusbrasil.com.br/artigos/169528179/crimes-contra-a-honra-na-internet Acesso em 2 fev. 2020.

NETTO FILHO, Dickson Cirilo Andrade. **Crime virtual:** crime contra o patrimônio no âmbito da internet, suas peculiaridades e controvérsias à luz do Código Penal de 1940. Âmbito jurídico. 2012. Disponível em: https://ambitojuridico.com.br/edicoes/revista-104/crime-virtual-crime-contra-o-patrimonio-no-ambito-da-internet-suas-peculiaridades-e-controversias-a-luz-do-codigo-penal-de-1940/. Disponível em: 28 maio 2020.

OLIVEIRA, Rafael. **Cinco tipos de crimes digitais devem dominar a internet brasileira em 2019**. 2019. Disponível em: https://www.jornalopcao.com.br/reportagens/cinco-tipos-de-crimes-digitais-devem-dominar-a-internet-brasileira-em-2019-212858/. Acesso em 10 mar. 2020.

OTOBONI, Gustavo Henrique dos Santos; ALMEIDA, Jeilton Frausto de; CAMPANHOLO, Matheus. **Crimes Cibernéticos:** Phishing. 2019. Âmbito Jurídico. Disponível em: https://ambitojuridico.com.br/edicoes/revista-191/crimes-ciberneticos-phishing/ Aceso em: 28 maio 2020.

PINHEIRO, Walber. **Crimes contra a honra:** investigação de publicações ofensivas na Internet. Blog IPOG. 2018. https://blog.ipog.edu.br/tecnologia/crimes-contra-a-honra-na-internet/

PIRES NETO, Lindolfo. **Crimes Cibernéticos:** necessidade de uma legislação específica no Brasil. 2009. Disponível em: http://www.fespfaculdades.com.br/painel/uploads/arquivos/trabArquivo_11052010080523_LINFOLFO.pdf. Acesso em 2 fev. 2020.

REDLER, Ivana. **Principais crimes contra o patrimônio**. Máster juris. 2019. Disponível em: https://masterjuris.com.br/principais-crimes-contra-o-patrimonio/. Acesso 28 maio 2020.

ROCHA, Adriano Aparecido. **Cibercriminalidade:** os crimes cibernéticos e os limites da liberdade de expressão na internet / Adriano Aparecido Rocha . – Garça, 2017.

SEGURADO, Rosemary; LIMA, Carolina Silva Mandú; AMENI, Cauê S. **Regulamentação da internet:** perspectiva comparada entre Brasil, Chile, Espanha, EUA e França. 2014. Disponível em: http://www.scielo.br/pdf/hcsm/2014nahead/0104-5970-hcsm-S0104-59702014005000015.pdf. Acesso em 3 mar. 2020.

SOARES, Samuel Silva Basilio. **Os crimes contra honra na perspectiva do ambiente virtual**. 2017. https://ambitojuridico.com.br/cadernos/direito-penal/os-crimes-contra-honra-na-perspectiva-do-ambiente-virtual/. Acesso 28 maio 2020.

SOUZA, Eric Henrique de. **Crimes digitais e evolução da legislação**. JusBrasil. 2017. Disponível em: https://ericmsouza.jusbrasil.com.br/artigos/420184154/crimes-digitais-e-evolucao-dalegislacao. Acesso em 8 fev. 2020.

TATEOKI, Victor Augusto. **Classificação dos Crimes Digitais**. Disponível em: https://victortateoki.jusbrasil.com.br/artigos/307254758/classificacao-dos-crimes-digitais. Acesso 28 maio 2020.

UOL. **Brasil é o segundo país no mundo com maior número de crimes cibernéticos**. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2018/02/15/brasil-e-o-segundo-pais-no-mundo-com-maior-numero-de-crimes-ciberneticos.htm. Acesso em 10 mar. 2020.