INSTITUTO VALE DO CRICARÉ
FACULDADE VALE DO CRICARÉ
CURSO DE DIREITO

LUCAS CARDOZO NOVAIS

CRIMES CIBERNÉTICOS E SUA EVOLUÇÃO

SÃO MATEUS
2020

LUCAS CARDOZO NOVAIS

CRIMES CIBERNÉTICOS E SUA EVOLUÇÃO

Trabalho de Conclusão de Curso apresentado do Curso de Direito, da Faculdade Vale do Cricaré, como requisito parcial para obtenção do grau de Bacharel em Direito.

Orientador Prof. Montalvan Antunes Rodrigues.

SÃO MATEUS
2020

LUCAS CARDOZO NOVAIS

CRIMES CIBERNÉTICOS E SUA EVOLUÇÃO

Trabalho de Conclusão de Curso apresentado ao Curso de Direito da Faculdade Vale do Cricaré, como requisito parcial para obtenção do grau de Bacharelado em Direito.

Aprovado em _____ de _____ de 2020.

BANCA EXAMINADORA

_____
___
PROF.º MONTALVAN ANTUNES RODRIGUES
FACULDADE VALE DO CRICARÉ
ORIENTADOR

_____
___
PROF.
FACULDADE VALE DO CRICARÉ

_____
___
PROF.
FACULDADE VALE DO CRICARÉ

SÃO MATEUS
2020

Dedico este trabalho aos meus pais, Lindinalva e Juvenil, que acreditaram na minha conquista, e nunca deixaram de me apoiar, pois sem eles não teria chegado até aqui.

AGRADECIMENTOS

Primeiramente a Deus por nada me deixar faltar, e toda gratidão do mundo aos meus pais, meu irmão, e todos os amigos que me apoiaram ao longo de toda esta fase.

.

Se alguém lhe disser que você não é capaz, tape os ouvidos e tente! Nem todos que tentaram conseguiram, mas todos que conseguiram aos menos tentaram.

Alexsandra Rios

RESUMO

O objetivo do presente trabalho se despende na necessidade de refutar a constante evolução tecnológica atual, onde milhares de computadores, smartphones, e os mais diversos dispositivos eletrônicos se interligam através de uma rede virtual, possibilitado uma informação de ponta a todo instante, comandos remotos, entre outros, e se tornam cada vez mais dependente de uma conexão de rede para o seu efetivo funcionamento, realidade condizente com a expansão vivida no século. Expõe um sucinto relato histórico sobre o surgimento e crescimento da rede mundial de computadores do Brasil e no mundo, e esclarece questões pertinentes. De uma forma direta serão trazidos assuntos relacionados aos cibercrimes e a forma em que os infratores agem para fraudar e lesar as suas vítimas. Levanta-se também a importância de uma lei que julgue especificamente sobre os crimes virtuais, e devida verificação se hoje existem projetos de lei que visam sobre o assunto, e com a devida punição para os transgressores.

Palavras-chave: Crimes Virtuais. Web, Crackers. Invasão a dados.

ABSTRACT

The objective of the present work is the need to refute the constant current technological evolution, where thousands of computers, smartphones, and the most diverse electronic devices are interconnected through a virtual network, providing cutting edge information at all times, remote commands, among others, and become increasingly dependent on a network connection for its effective functioning, a reality consistent with the expansion experienced in the century. It presents a succinct historical account of the emergence and growth of the worldwide computer network in Brazil and in the world, and clarifies pertinent questions. In a direct way, issues related to cybercrimes and the way in which offenders act to defraud and harm their victims will be brought up. It also raises the importance of a law that specifically judges on cyber crimes, and due verification if today there are bills that target the subject, and with due punishment for offenders.

Keywords: Virtual Crimes. Web, Crackers. Data invasion

SIGLAS E ABREVIATURAS

ART – Artigo

CBT – Código Brasileiro de Telecomunicações

CF – Constituição Federal de 1988

CP – Código Penal

PL – Projeto de Lei

PLC – Projeto de Lei da Câmara

PLS – Projeto de Lei do Senado

IP - Endereço de Protocolo da Internet, do inglês Internet Protocol address

WAN – *Wide Area Network*

WWW – *World Wide Web*

VPN – Rede privada virtual

ISP – Um Fornecedor de Acesso à Internet ou Provedor de Serviço Internet

IP – Endereço de Protocolo da Internet

STJ – Superior Tribunal de Justiça

LAN HOUSE – *E*stabelecimento comercial que se associa a cybercafé

MAWALRES – *S*oftware nocivo ou mal-intencionado

ECA – Estatuto da Criança e do Adolescente

PHYSHING – Tentativa fraudulenta de obter informações confidenciais

SMS – Serviços de Mensagens via Celular

WI-FI – Rede de Internet sem fio

SUMÁRIO

1 INTRODUÇÃO

O Direito se tornou presente em todo e qualquer momento da vida de um indivíduo que conviva em um regime de estado democrático, como é o modelo atual vivido no Brasil, pois somente através do Direito torna-se possível a resolução de conflitos impostos pela sociedade, onde está mesma não consegue administrar seu próprio crescimento diário, e vem a ocorrer em ritmo acelerado, advindo de descobertas e aprimoramentos tecnológicos, que visam tornar a vida da humanidade cada dia mais fácil e simples.

Entretanto, com o desenvolvimento desenfreado perante ao campo tecnológico, onde abrange o ramo da internet de forma genérica, alguns indivíduos que praticam condutas delituosas de forma virtual, tornam-se difíceis de se rastrear, e até mesmo sofrerem uma punição de acordo com a proporção do delito causado.

A concretização dessa pesquisa se baseia na necessidade do conhecimento sobre a utilização correta das leis no âmbito virtual, principalmente sobre o olhar da comunidade jurídica da área do direito penal, e assim transpor todos e quaisquer impactos que podem causar na vida da sociedade.

Dentre os crimes virtuais que alastram diariamente, destaca-se o crime de estelionato, onde cresce o número de vítimas diariamente, onde os delituosos analisam o perfil da sua vítima, onde na maioria das vezes não se faz distinção de classe financeira, e assim lhe causando um prejuízo moral ou financeiro.

Com a modernidade e o avanço da tecnologia, a sociedade se torna a cada dia mais dependente de um equipamento eletrônico conectado à rede mundial de computadores (Internet), sendo ele para facilitar a comunicação com qualquer parte do mundo, ou até mesmo para simplificar tarefas do dia a dia.

A lacuna causada pela ausência de uma lei especifica para tratar diretamente do assunto faz com que aumente diariamente o número de

criminosos, pois a legislação ainda é antiquada ao tempo atual, onde a mesma não é compatível com os novos crimes sofridos pela sociedade.

Somente em 2012 após uma atriz famosa ter suas fotos intimas vazadas na internet, a atual presidente na época Dilma Rousseff, sancionou a Lei 12.737/2012, muito conhecida como Lei Carolina Dieckmann, onde tipifica algumas curtas condutas no âmbito virtual.

Por fim, serão tragos no decorrer deste, as leis existentes que já decorrem sobre o assunto, por vertente especifica ou por analogia, e também, será abordado sobre os projetos de lei acerca do assunto, onde os mesmos já tramitam aguardando analise e possíveis alterações, até chegar a sua aprovação.

2 CRIMES VIRTUAIS

Grandes autores costumam utilizar o termo “aldeia global” para se tratar sobre a então chamada globalização, que veio a dar início no século XV, durante o período mercantilista, período em que nações europeias se lançavam ao mar na busca de terras, e grandes riquezas para seu povo.

Ao longo dos séculos, sendo decorrido de novas invenções como por exemplo a eletricidade, novos horizontes foram abertos, fazendo com que o homem chegasse a conquistas inimagináveis para a época.

Nas palavras do professor Boaventura de Souza Santos (1997), a globalização se baseia em um fenômeno centrado na economia mundial, sendo sustentada por empresas multinacionais.

A globalização é o processo pelo qual determinada condição ou entidade local consegue estender sua influência a todo o globo e, ao fazê-lo, desenvolve a capacidade de designar como local outra condição social ou entidade rival (SANTOS, 1997, p.108).

Com esse fenômeno crescendo demasiadamente, foram se expandindo também as diversas mudanças significantes, tanto na área política, jurídica e social, onde se exige a busca pelo Direito, onde tem o intuito de se moldar e compreender esse crescimento, e impedir que a sociedade digital venha a se tornar a margem do controle estatal.

A tecnologia veio se tornando o epicentro de todo esse avanço tecnológico do século, se fazendo insustentável viver sem a devida regulamentação para seus usuários, para que seja possível se criar um ambiente virtual sustentável e desenvolvido.

A internet se tornou a maior ponte para toda a desenvoltura tecnológica, pois através dela ligando ponta a ponta do mundo, tornou-se possível levar novas tecnologias de informação e o crescimento social para muitas culturas.

Por outro lado, cresce também a utilização desse importante meio tecnológico para a prática de atos ilícitos (TRENTIN; TRENTIN, 2012).

Com todo esse crescimento demasiado, torna-se como dever de o Estado fazer com que se cumpra a o direito a um crescimento igualitário de toda a sua população, e se mantendo no centro e no controle da ordem social. Dessa forma acaba por interferir no âmbito virtual da sociedade, ao impor limites a seus usuários.

Em âmbito Mundial, enquanto diversos países desenvolvidos buscavam agilizar todo o processo da criação de uma legislação eficiente, com no qual as normas da internet se tornassem eficientes, o Brasil permaneceu levando o assunto de uma forma mais lenta, onde veio a promulgar leis para tratar da regulamentação da internet, e se tornando como prioridade a proteção de temas como a liberdade de expressão, direitos do consumidor e crimes virtuais (PINHEIRO, 2014).

Os crimes cibernéticos existem desde o início da internet, e no Brasil não se tornou diferente, mas somente em 18 de junho de 1996 se tornou registrado o primeiro crime cibernético brasileiro. A notícia se tornou pública quando foi descoberta uma invasão em vários sites ligados ao governo, como o site oficial do Supremo Tribunal Federal, e partir deste evento a sociedade brasileira soube pela primeira vez o que seria o início dos crimes cibernéticos, e o governo passou a ter esta invasão cibernética como seu primeiro problema virtual, e sem qualquer plano imediato para apresentar como solução.

Com base em dados fornecidos pela AVG (Empresa produtora de Softwares Antivírus), onde consta em seus registros que o crime cibernético apenas se tornou constante no Brasil após o ano de 2002, e tendo como principais vítimas clientes bancários, onde os criminosos agem retirando pequenas quantias da conta dos clientes, na maior parte da vezes (centavos), que se torna de difícil percepção do cliente e da agência bancária, sendo o crime repetido em mais de um cliente, e por diversas vezes consecutivas.

Relata-se como exemplo um julgado de 2007, do Superior Tribunal de Justiça (GO (2006/0166153-0), onde foram retiradas pelos crackers quantias da conta do cliente, que possuía conta na Agencia da Caixa Econômica Federal, e ao final totalizou o montante de R$2.525,15 (dois mil e quinhentos e vinte e cinco reais e quinze centavos) de prejuízo.

O Grande Marco Civil da Internet, como assim ficou conhecida a LEI 12.965/2014, foi promulgada com o intuito principal de regular o uso da internet no Brasil, tendo como base a previsão de princípios, garantias, direitos e deveres para os usuários da WEB. O projeto inicial da lei surgiu no Governo da Ex Presidente Dilma Rousseff em 2007, onde o projeto seguiu em forma de debate aberto em forma de um blog digital, e foi comentado pelos internautas, onde foram feitas sugestões a respeito do projeto.

Anteriormente a este projeto, foi sancionada em 2012, também no Governo da então Ex Presidente Dilma Rousseff, a Lei 12.737, onde veio para introduzir no código Penal Brasileiro os artigos 154-A e 154-B.

Um criminoso informático diferentemente de indivíduo que pratica um “crime real” torna-se perigoso e difícil localização, pois ao mesmo tempo pode cometer mais de uma conduta criminosa simultaneamente, atingido suas vítimas de qualquer local, e age de forma silenciosa, tornando na maioria das vezes a vítima sem defesa e sem reação, e dispensando qualquer tipo de violência ou contato físico.

Considera-se também que para alguns usuários a WEB acaba se tornando um ambiente familiar, onde está presente a todo momento, aumentando a sensação de segurança e anonimato, e acaba abaixando a guarda, deixando muitas vezes dados expostos, sem qualquer proteção de antivírus ou bloqueadores de malwares.

Torna-se inimaginável a ideia de que se pode parar em um detector de metais um assaltante de banco, mas não se consegue controlar um criminoso que age de forma virtual em agências bancárias, seja do governo ou de

instituições privadas, onde por exemplo pode se mencionar o Hacker que no dia 24/08 desse mesmo ano foi preso no estado de Santa Catarina, por desviar mais de R$648 mil reais de contas de clientes de uma instituição bancária

Direito Informático e o Direito Penal no Brasil mesmo com toda a evolução, permanece como área tão pouco explorada, existe uma vaga originalidade doutrinária nos projetos de artigos brasileiros, onde não se existe um conhecimento técnico aprofundado do conteúdo virtual e um entendimento compreensível da língua estrangeira, e no fim o que acaba se tornando é um projeto parcial do ordenamento de outros países.

Em um âmbito geral, a rede mundial de computadores trouxe para a sociedade o Princípio da Igualdade, ou da Isonomia, onde tornas seus usuários sem qualquer distinção de classe, raça ou qualquer outro fator. De forma igual se pensava Aristóteles, onde na sua concepção de Estado, deveria ser exigido quando mencionado o termo Estado, que todos os indivíduos da sociedade fossem tratados de forma igual.

2.1 DEFINIÇÃO DE CRIMES VIRTUAIS

No momento em que a criminologia percebeu que a internet se tornaria um novo foco de criminalidade, tornou-se necessária a criação de teorias para definir os crimes virtuais, bem como entender por qual razão eles ocorrem (JAISHANKAR, 2007)

No Brasil, a infração penal pode ser dividida entre gêneros, podendo ser caracterizado como um crime (ou delito), ou contravenção penal (também conhecido como crime anão ou crime vagabundo). Sendo rotulado pelo legislador as condutas mais graves como crime, e as de menor potencial com menos lesividade como contravenções penais. (CUNHA, 2014).

Guilherme Nucci (2011, p. 173) conceitua a sua análise sobre crime e contravenção penal da seguinte forma:

Poucos institutos sobreviveram por tanto tempo e se desenvolveram sob formas tão diversas quanto o contrato, que se adaptou a sociedades com estruturas e escala de valores tão distintas quanto às que existiam na Antiguidade, na Idade Média, no mundo capitalista e no próprio regime comunista (2000, p. 43).

Não se existe um consenso entre os doutrinadores que abordam o tema e a sua complexidade, onde todas as ideias envolvem-se em abarcar condutas realizadas através de variados dispositivos tecnológicos, onde o termo usado nesse trabalho será “Crimes Virtuais”.

O professor Paulo Marco Ferreira Lima define os crimes virtuais, como (crimes de computador), e como uma conduta caracterizada aos olhos do direito penal como fato típico, antijurídico e culpável, em que a máquina (computador), tenha sido utilizada, como meio facilitador para a consumação da ação delituosa, e vindo a causar prejuízos a sociedade, vindo a trazer benefício ou não ao autor do ato. (PALAZZI, 2000).

Existem relatos que os primeiros crimes virtuais foram registrados na década de 1970, onde os grandes especialistas da área da computação e informática tinham como objetivo de burlar sistemas de segurança de bancos. Nos dias de hoje a forma de ação dos criminosos não mudaram, mas somente o perfil do criminoso dever ser analisado com mais cautela, pois o o acesso se tornou mais amplo, e o indivíduo pode praticar o seu delito de dentro de casa, sem precisar do uso de grandes ferramentas, sendo basicamente um ‘usuário doméstico’.

É possível caracterizar os crimes virtuais de duas formas, sendo divididos como crimes próprios ou impróprios. Os primeiros, possuem como intuito o atingir um sistema informático, onde ataca os dados do usuário, violando sua confiabilidade, sua integridade ou sua disponibilidade. Os segundos, são condutas comuns e também antijurídicas, que perpetuam do uso de ferramentas

informáticas, mas que poderiam ter sido praticadas por outros meios. (SYDOW, 2014).

Fabrízio Roza (2007, p. 53), ao tratar da denominação envolvendo crimes cibernéticos, bem pontua que “Klaus Tiedemann fala em ‘criminalidade de informática’ para designar todas as formas de comportamentos ilegais ou, de outro modo, prejudiciais à sociedade, que se realizam pela utilização de um computador.

Neste posicionamento Tiedemann visa por um lado os problemas vividos por um indivíduo da esfera privada, que possa ter sua integridade ameaçada pela interconexão de dados, e por outro lado, visa-se os danos ao patrimônio cometidos através da web.

No Brasil os crimes virtuais ganharam um nome, ficando conhecido pelo mundo jurídico como “delitos informáticos”, terno esse já utilizado por países como a Espanha, que traz por derivação a ideia de preserva e proteger o bem jurídico, sendo ele a própria rede ou informações contidas nela. Como grandes exemplos de crimes virtuais, pode se citar o estelionato, pornográfica infantil e não menos importante, os ataques por physhing, onde a vítima acaba vindo a se sentir atraída por um anuncio na web ou até mesmo uma mensagem sms, onde vem carregado com um malware que se instala na máquina do usuário, e tem como ação principal o roubo de identidade da vítima.

3 CRIMES POR MEIO ELETRÔNICO E REDE

Como já mencionado anteriormente, localizar um criminoso ou o local usado para a pratica de um crime virtual pode vir a se tornar uma tarefa praticamente impossível, pois infratores não sofrem com barreiras ou qualquer bloqueio para impedir suas ações, possuem carta branca para trafegar por toda rede global de comunicação mundial.

Nos últimos 20 anos as pessoas têm passado cada vez mais tempo conectadas na Internet, e por consequência os crimes cometidos no ambiente virtual também cresceram (CELLA, 2012).

Crimes cometidos contra um sistema de computadores, onde interligados a rede por um provedor de internet se conectam a um mundo de informações, podem ser praticados de qualquer lugar do mundo, a vítima estando longe ou próxima do autor, e não atingindo somente computadores, mas qualquer equipamento eletrônico que esteja compartilhando da rede, sendo ele, um smartphone, entre outros.

Parte destas ações delituosas ocorrem tanto pela rede quanto pelo mundo real, porém alguns crimes sofrem peculiaridades especificas, sendo o que torna necessário uma adequação quanto ao seu tipo penal.

3.1 INVASÃO À PRIVACIDADE

A rede mundial de computadores traz para o seu usuário o conforto e comodidade de fazer praticamente qualquer coisa sem se levantar, sendo para uma compra ou até mesmo para se mantar informado em uma página de notícias ou nas redes sociais, mas para que isso aconteça com fluidez, as páginas e sites na grande parte das vezes, pede para que o seu usuário faça um cadastro ou simplesmente que crie um loguin para acesso a plataforma, e com essa participação dos usuários, foi crescendo a circulação de dados de forma eletrônica, onde ao preencher até mesmo um questionário os dados do cliente são expostos para criminosos.

Pessoas físicas ou jurídicas têm o direito à intimidade e privacidade, à segurança da informação, e este direito se estende ao que se encontra em seus dispositivos informáticos. Daí por que a Lei n.12.737/2012 exige que mantenhamos incólumes tais dispositivos informáticos, sobretudo seu conteúdo, por meio do tipo penal que é inserido no Decreto-Lei n. 2.848/40 dentre os crimes contra a liberdade Individual, a seguir citado:

> 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.

A Constituição Federal no seu artigo 5º, X, garante a proteção da privacidade, garantindo ao cidadão o direito a reparação ao ter sua privacidade violada, onde diz:

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

X - São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

No âmbito jurídico visa-se a necessidade de preservar a privacidade e liberdade do indivíduo, e principalmente a proteção de seus dados, e qualquer informação a torno dela que circule na web. Com as palavras de Marcio Cavalcanti (2013, p.1) onde diz:

“O bem jurídico protegido é a privacidade, gênero do qual são espécies a intimidade e a vida privada”.

No direito, tutela-se a liberdade individual com a finalidade de manter a integralidade dos dados inseridos no meio informático, de uma forma simples, onde nos casos confirmados o intuito desse acesso a informação é para obter dados do usuário, alterar estes dados obtidos, ou até mesmo destruir para

causar um prejuízo moral ou financeiro, ou instalar a vulnerabilidade e assim obter vantagem ilícita, sendo financeira ou não.

A lei existente determina como condição inicial para se qualificar a prática do delito, que o dispositivo invadido esteja protegido por uma medida de segurança a altura, ou seja, fora dos padrões de fábrica geralmente estabelecidos. Como porta de entrada no acesso a rede, o moldem e roteadores são os primeiros atingidos, abrindo caminho para a pratica do delito, e neste caso pode ser caracterizada a atipicidade do fato se o mesmo estiver com as senhas padrões de fábrica (admin ou 123, entre outras), pois os juristas caracterizam que a falta de segurança ou proteção conduz a atipicidade do fato, e que a sua ineficácia é o que equivale a sua ausência.

Mas entretanto, existem correntes contrárias, que advogam a favor de que pelo simples fato de existir uma barreira ou proteção, por mais simples que seja, já configura o delito, deixando de lado se a proteção era eficaz ou não.

Não há de se haver uma confusão entre proteção e gravação, onde usa-se como exemplo um cartão de memória ou pen drive, que possui informações do usuário, e caso esse usuário venha a perder este dispositivo e um indivíduo o encontre e faça uso destas informações, não poderá caracterizar como “invasão”, já que houve um descuido do proprietário e facilitou o acesso por terceiros, mas não deixando a conduta de ser caracterizar como crime, onde o autor do delito poderá responder pelo (crime de dano, previsto no art. 163 do Código Penal), e caso a posse do dispositivo tenha sido mediante furto, responderá também com base no (art. 155 do Código Penal).

Por um outro lado da mesma doutrina, segue se o raciocínio de que se o dispositivo (pen drive ou cartão) estiver sido furtado de um cofre em segurança, que poderá se caracterizar o crime em questão, (Invasão a dispositivo informático – art. 154-A do Código Penal).

Neste caso dispensará qualquer medida protetiva no dispositivo, como firewall ou demais softwares, pois próprio cofre já servirá como medida de segurança, mesmo sendo de forma externa, não sendo por meio eletrônico.

3.2 ESPIONAGEM ELETRÔNICA

No campo da espionagem eletrônica o Brasil se encontra com um dos maiores atrasos mundiais, utilizando como base a Espanha, onde em 2006 o governo propôs uma atualização da legislação vigente especificamente para este crime.

Considerando que até a criação da Lei 12737/2012 a única Lei que o Brasil tinha a respeito de Crimes Virtuais ela a Lei 9.983/000, onde se dirigia especificamente a crimes informáticos praticados por servidores públicos.

O Código Penal não possui uma tipificação de forma especifica para o crime de espionagem eletrônica, sendo definida somente pelos artigos 154 e 154A.

Perante o âmbito das instituições privadas, regidas pela CLT, seguem o art. 482 da CLT, onde diz que poderá ser rescindido o contrato de trabalho e o trabalhador dispensado por justa causa, com base na alínea “a”:

> Art. 482 - Constituem justa causa para rescisão do contrato de trabalho pelo empregador:
> a) Ato de improbidade;

3.3 FRAUDES VIRTUAIS

O crime de fraude eletrônica foi reconhecido a partir do ano de 2012, onde houve a criação e aprovação da a apelidada “Lei Carolina Dieckmann”, projeto de Lei “12.737/2012), o intuito principal desta lei foi atender uma demanda antiga do setor financeiro, o qual é impactado diretamente pelas fraudes eletrônicas,

gerando prejuízos irreparáveis, e pelo fato desta lei ter sido aprovada as pressas diante do ocorrido a atriz Carolina Dieckmann, tornou-se uma lei circunscrita, quando se leva em comparação com os demais projetos existentes que tramitam no Congresso Nacional.

Entende-se que aprovar uma lei menor, onde não traga tantos assuntos polêmicos, onde a causa principal seja somente regular algo a respeito de crimes cibernéticos, é como o ditado em que diz, que a lei é como remédio, deve ser ministrado em doses, pois se ministrarmos tudo de uma vez, podemos matar o paciente. (Damásio, José , 2014).

De acordo com o CERT-BR (Centro de estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil), define-se que fraude eletrônica se dá pelo recebimento de mensagens recebidas não solicitadas, onde se passam por instituições conhecidas, ou também utilizam a tática de persuadir o usuário com mensagens que o induzem a clicar em links maliciosos, compostos com códigos que se instalam, advindos de origem duvidosa.

Existem duas modalidades de fraudes virtuais, sendo conhecidas como fraudes externas e internas. As fraudes externas ocorrem quando quem comente o crime não possui vinculo direito com o local a ser fraudado, e a fraude interna fica sendo cometida quando o infrator possui vínculo com o local a ser fraudado podendo vir a ser desde um empregado, morador, ou até mesmo um prestador de serviço que passou pelo local.

3.4 CRIMES CONTRA A HONRA

A honra do indivíduo não estar ligada somente a sua posição social, mas diz respeito a sua boa fama perante a sociedade, sentimento interior e a sensação de estar em paz com a própria consciência.

Entre o conjunto de atributos interligados a honra do indivíduo, vale salientar que a honra pode ser atingida de forma objetiva, quando se equivale ao juízo que terceiros fazem acerca de atributos de uma pessoa. A honra também

pode ser atingida de forma subjetiva, que se compara ao pensamento da própria pessoas sobre seus próprios atributos.

Os crimes contra a honra estão compostos diretamente na vida de grande parte dos usuários da web, na grande parte das vezes até acaba passando despercebido aos olhos. O rol de crimes contra a honra é composto e subdivididos entre a Calúnia, Difamação e Injúria, neste primeiro ponto falar do primeiro deles, o qual é calunia, disposto no art. 138 do Código Penal, onde diz:

Caluniar alguém, imputando-lhe falsamente fato definido como crime.

A difamação é considerada pelos juristas o crime mais comum praticado via web, onde se ataca diretamente a sua honra objetiva, sendo imputando a vítima um fato ofensivo a sua reputação, este crime se encontra no Art. 139 do Código Penal, onde diz:

> Art. 139 Difamar alguém, imputando-lhe fato ofensivo à sua reputação:
> Pena – Detenção, de 3 (três) meses a 1 (um) ano, e multa.

Já no crime de Injúria, o autor atribui de forma negativa uma qualidade da vítima, onde está ligada a seus atributos morais, intelectuais, ou físicos, e tende a ofender diretamente a honra subjetiva da vítima. Crime previsto no Art. 140 do Código Penal, onde diz:

> Art. 140 Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:
> Pena - detenção, de um a seis meses, ou multa.

3.5 PORNOGRAFIA INFANTIL

De acordo com (CID-10/OMS), Classificação Internacional de Doenças, a pedofilia se atribui um ato de perversão de um indivíduo adulto a sentir atraído por crianças ou adolescentes, geralmente pré-purberes ou no início da puberdade, e sentir interesse em praticar atividade sexual com a mesma.

Partindo da premissa pedofilia, nasceu a pornografia infantil, onde tornou-se um crime que se popularizou em todo mundo, e após a expansão da internet, se tornou um crime em evidencia, e veio a se tornar uma conduta analisada por psicólogos e juristas.

A pornografia infantil, baseia-se no conceito de expor uma criança ou adolescentes por meio de fotos ou vídeos, onde exponha seus órgãos sexuais, ou que simplesmente o menor esteja em posições de sensualidade, não sendo nesse caso necessário que haja a nudez para caracterizar o fato.

Para a pornográfica existir, não é necessário que se haja uma relação antes, como existe na pedofilia, onde basta somente que o indivíduo divulgue ou comercialize material erótico, ou de cunho sexual, que envolta crianças ou adolescentes. O Código Penal no seu Art. 234, diz:

> Art. 234 Fazer, importar, exportar, adquirir ou ter sob sua guarda, para fim de comércio, de distribuição ou de exposição pública, escrito, desenho, pintura, estampa ou qualquer objeto obsceno:
> Pena – detenção, de 6 (seis) meses a 2 (dois) anos, ou multa.

Com base no entendimento do STJ, entende-se que:

É típica a conduta de fotografar cena pornográfica (art. 241-B do ECA) e de armazenar fotografias de conteúdo pornográfico envolvendo crianças ou adolescentes (art. 240 do ECA) na hipótese em que restar incontroversa a finalidade sexual e libidinosa das fotografias, com enfoque nos órgãos genitais das vítimas – ainda que cobertos por roupas-, e de poses nitidamente sensuais, em que explorada sua sensualidade com conotação obscena e pornográfica.

De acordo com os registros, os crimes de pornografia infantil começaram a ser registrados na década de 90, logo após ter sido criado o primeiro vírus de computador conhecido.

Logo mais em 1998, o Ministro do Supremo Tribunal Federal, Sepúlveda Pertence, deu aula ao falar sobre o HC 76.889/PB, caso esse que envolvia pornografia infantil, e com suas palavras o Ministro disse:

“Nem todos os delitos cibernéticos necessitam de nova tipificação, eis que em muitos a tecnologia é só um novo meio utilizado para concretização de delitos conhecidos. ”

3.6 ESTELIONATO

Dos crimes mais novos até os mais antigos o estelionato se encontra presente, estando entre os crimes comuns praticados. No campo da informática o estelionatário.

De acordo com o entendimento de grandes juristas, hoje existe a necessidade de se alterar o artigo 171 do Código Penal, onde seria incluído o crime para que praticasse o estelionato de forma virtual, e a pena viria a ser a mesma do *caput.*

O estelionato praticado por meio de meio eletrônico encaixa-se, perfeitamente, no tipo penal estabelecido pelo artigo 171 do Código Penal, sendo possível sua aplicação sem maiores ressalvas (CAPEZ, 2016).

> Art. 171. Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento.
> Pena – reclusão, de 1 (um) a 5 (cinco) anos, e multa.

O estelionato veio a se tornar um dos crimes mais populares do ordenamento jurídico, e com o uso da internet o número de pessoas que tendem a querer obter vantagens ilícitas para si ou para outro só tendem a crescer.

No estelionato virtual é de natureza do criminoso enviar um link malicioso para um usuário aleatório, onde faz com que esse usuário acredite que ao clicar naquele link será redirecionado para uma página confiável afim de atualizar ou criar um novo loguin cadastral, tendo assim um caminho aberto para obter todas as informações confidenciais disponíveis que o usuário vir a fornecer.

Existem algumas possibilidades de ajudar o usuário a se livrar desses e-mails e links spam, onde com base em informações da própria Microsoft a principal medida é sempre manter o sistema operacional rodando com a última atualização disponível, e sempre que possível instalar antivírus confiáveis, e de grande importância são os bloqueadores de malwares, que filtram as informações recebidas, e bloqueiam os anúncios indesejados e maliciosos, tornando a navegação mais segura.

4.0 CRIMES VIRTUAIS NA LEGISLAÇÃO VIGENTE

Neste capitulo será feita uma análise a respeito da legislação vigente acerca dos crimes virtuais, e também será tratado a respeito de projetos de lei que já estão em tramitação Câmara dos Deputados e Senado Federal.

Para muitos doutrinadores, dados ou informações não poderiam ser subtraídos, diga-se, saírem da esfera de disponibilidade da vítima, nem mesmo ser objeto de destruição (considerando que comumente dados são copiados indevidamente). Para outros, ainda que intangíveis, dados, por terem relevância econômica, tal como a energia elétrica, mereciam a relevância do ordenamento jurídico penal.

Em junho de 2006, Tim Berners- Lee conhecido com um dos fundadores da internet, contrariando o pensamento dos juristas, alegou que não há necessidade de se ter uma legislação especifica para crimes na internet, pois ao

seu ponto de vista, no passado não foi necessário, e no presente também não faria falta, e finalizou com a ideia, de que essa legislação caso criada, atingiria a liberdade dos usuários.

Na visão do Direito como ciência humana, afirma-se que não existe condições de se ficar para trás no marco de avanços da internet, afinal, são as leis que estabelecem os direitos dos usuários da internet.

Marcos civis regulatórios da Internet são apontados como fatores para o fortalecimento de uma sociedade na era da informação, em suas múltiplas dimensões, social, cultural e econômica, e vêm sendo estudados em todo o mundo (CARVALHO, 2014).

O Brasil de outra forma, optou por seguir o caminho contrário, onde adota-se primeiramente a legislação criminal (legislação está que deveria ser última ratio), de modo a punir condutas praticadas por intermédio ou contra sistemas informáticos.

Surgiu a Lei n 9.609/98, sancionada em 19 de fevereiro de 1998, que veio para substituir a lei 7646/87, que seria completamente ultrapassada para a época em questão e única vigente até então.

A proposta da nova legislação, seria de trazer um conceito inovador acerca do âmbito virtual, mas seu real intuito seria de proteger os direitos intelectuais de programadores, criadores de programas e softwares de computadores, tratar a respeito da comercialização desses programas criados e tomar demais providencias.

Somente 14 anos após a criação desta última lei, foi analisada pelo Congresso Nacional a necessidade de uma legislação por mais simples que fosse, para vigorar sobre os crimes informáticos, afinal diariamente novos crimes surgiam, e a cada dia mais se usava a legislação penal a seu respeito.

A partir desta necessidade, foram criadas as leis 12.735/12 e 12.3737/12 que foram publicadas com o interesse de alterar o Código Penal para também tratar de crimes virtuais.

A Lei 12.735/12, surgiu com a necessidade de tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra informatizados e similares; e dá outras providências.

Esta Lei trouxe 23 artigos no projeto inicial, mas 19 sendo vetados pela Ex Presidente Dilma Rousseff, vindo somente 4 a serem sancionados e somente 2 tendo conteúdo penal.

Também em 2012 foi sancionada a Lei n 12.737/12, que veio a ser apelidada de “Lei Carolina Dieckmann”, posteriormente sendo criada com base no crime sofrido pela atriz Carolina Dieckmann, onde fotos intimas da atriz foram divulgadas, e demais arquivos foram subtraídos de seu dispositivo, mediante um e-mail com link de spam que a atriz veio a receber, e seguidamente clicou no link malicioso, permitindo a instalação do vírus, e facilitando para que os criminosos tivessem acesso a sua caixa de e-mails.

Esta lei foi criada com o fundamento de tipificar delitos informáticos e dá outras providências.

Ainda nos dias de hoje a eficácia da lei 12.373/12 circula entre os doutrinadores, pois sua criação veio após um caso especifico, tornando sua tutela individual, e envolvendo somente os interesses particulares de pessoas (físicas ou jurídicas), não tendo impacto direto como normativa para a proteção da rede de computadores.

Salienta-se que a Lei 12737/12 se tornou longe de controlar determinadas situações, isso porque a punição do delito somente tange quando for praticado com a finalidade dolosa, deixando de importar o resultado desta atividade.

Em termos sociológicos foi fator determinante à aprovação da Lei 12.737/2012 a ocorrência de escândalos reiterados de vazamento de fotos íntimas que passaram a afetar um número cada vez maior de pessoas, fazendo com que houvesse uma pressão social cada vez maior sobre o legislativo para que houvesse o endurecimento das penas envoltas à este tipo de delito. (BARBOSA et al, 2014).

Assim na sociedade da informação, busca-se a cada dia proteger direitos supra individuais, em um modelo de prevenir os riscos do estado, e não contra ameaças existentes na sociedade, tornando-se desprotegido o bem jurídico.

A referida lei abre a opção de que não precisa ser exatamente o proprietário de um computador para ser caracterizado o crime de violação caso esse dispositivo seja invadido, todo terceiro envolvido na relação também se tornara vítima.

Como por exemplo, se um usuário tiver seus dados violados através de um dispositivo de uma lan house, o proprietário da mesma também se torna uma vítima, pois a fraude aconteceria através de seu dispositivo, vindo o mesmo a ter sua rede aberta por esses criminosos.

Em 2014 foi criada a lei que passaria a ser conhecida como o “Marco Civil da Internet”, sendo ela a Lei n 12.965/2014, onde passou a regular o uso da internet em todo o território brasileiro, por meio da previsão de princípios e garantias, direitos e deveres para os usuários da rede web, determinando também a forma de atuação do Estado.

A lei do Marco Civil foi criada para suprir as lacunas no sistema jurídico em relação aos crimes virtuais, num primeiro momento tratando dos fundamentos, conceitos para sua interpretação e objetivos que o norteiam, além de enumerar os direitos dos usuários, tratar de assunto polêmicos como por exemplo a solicitação de histórico de registros, a atuação do poder público perante os crimes virtuais e por último garante o exercício do direito do cidadão

de usufruir da internet de modo individual e coletivo estando devidamente protegido. (SIQUEIRA, 2017, p. 126)

Logo em seus primeiros artigos são apontados os princípios, objetivos e conceitos aplicáveis a matéria digital.

Destaca-se os princípios mencionados em seu art 3º.

> Art. 3º 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. (Planalto.gov.br)

O Marco Civil da Internet pode ser caracterizado como uma vitória para os internautas e toda sociedade brasileira, pois teria chegado ao fim o apelo feito em 2009 pela sociedade para uma punição mais dura em relação aos crimes virtuais.

Com o advento do sancionamento da Lei 12.965/2012 trouxe para os provedores de internet uma nova obrigação que não existia, que seria a de

armazenarem os logs e dados de conexão dos usuários, pelo prazo mínimo de 3 (três) anos, onde deveria ser armazenado os dados endereços de IP, data, hora de início e termino da conexão e origem da chamada, está recomendação foi feita diretamente pelo Comitê Gestor de Internet do Brasil e um posicionamento do Superior Tribunal de Justiça (STJ).

Quando o usuário se conecta a internet para qualquer finalidade, faz através de um provedor de acesso, ou de um ISP (Internet Service Provider), e este provedor vem a lhe atribuir um endereço de IP (Internet Protocol), onde fica definido a data e hora de acesso, de acordo com a duração da conexão.

Deste modo o registro de IP do usuário facilita para a polícia em caso de investigação (caso não tenha mascarado a conexão), pois diversos criminosos utilizam de VPN's para burlar o endereço de IP, fazendo com que o mesmo seja redirecionado para a região do mundo em que desejar, tornando ainda mais difícil para a realização de uma investigação.

E através da operadora de internet é obtido os nomes dos usuários responsáveis pela conexão, bem como CPF, CNPJ, Nome e Endereço, tudo isso através do cadastro feito na adesão do plano feito pelo cliente na contratação do serviço.

Desta forma é possível haver um cruzamento de dados e se chegar até um responsável por a autoria de um delito cometido de forma virtual, onde geralmente os criminosos não são os titulares da conta, respondendo em partes o titular da conta por negligência, por permitir que determinados atos fossem praticados através de sua conexão, como ocorre com pessoas que costumam deixar redes WI-FI desprotegidas sem senhas, facilitando o acesso do cracker.

Com o Marco Civil sancionado, de acordo com o Inciso l do art. 7º, os usuários passaram a ter direito a inviolabilidade e sobre o sigilo de suas comunicações pela web, exceto quando for feita a solicitação por ordem judicial, para fins de investigação criminal ou instrução penal.

Se tornou extinta a possibilidade antes havida de se obter grampos informáticos na esfera civil, quando do processo de discorrer de fraude, concorrência desleal, dentre outros.

Em uma análise sucinta do artigos 13 e 15 do Marco Civil, fica definido por lei que os provedores de acesso (conectam o usuário a internet), deverão armazenar os registros de conexão dos usuários pelo prazo mínimo de 1 (um) ano, e da mesma forma os provedores de aplicações (serviços de utilidades da Internet) deverão armazenar os dados advindos de aplicações pelo prazo mínimo de 6 (seis) meses, sendo que os dados deverão se manter protegidos e em sigilo, e somente ser fornecidos por ordem judicial, e através de solicitação de autoridades administrativas, como Polícia e Ministério Público. Os seguintes artigos preveem:

> Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.
>
> 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.

Tornou-se um assunto polêmico o fato do Ministério Público não requerer diretamente aos provedores de internet um registro necessário, onde existe a necessidade que a quebra de sigilo seja autorizada através de pedido judicial.

De acordo com a Lei complementar n 75, de 20 de maio de 1993, que prevê as atribuições do Ministério Público da União:

> Art. 6º Compete ao Ministério Público da União:
> (...)
> XVIII – representar;
> a) ao órgão judicial competente para quebra de sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, para fins de investigação criminal ou instrução processual penal, bem como manifestar-se sobre representação a ele dirigida para os mesmos fins;

Com intenção de tornar o processo mais célere, foi criada a Lei n 12.683/12, com o fundamento de dar a autonomia ao Ministério Público e a Polícia para solicitar a empresas telefônicas, provedores de internet e empresas de cartões de credito, dados cadastrais, filiações e endereços de investigados em crimes de lavagem de dinheiro, independentemente de autorização judicial. O Art. 17-B da Lei dispõem:

> Art. 17-B A autoridade policial e o Ministério Público terão acesso, exclusivamente, aos dados cadastrais do investigado que informam qualificação pessoal, filiação e endereço, independentemente de autorização judicial, mantidos pela Justiça Eleitoral, pelas empresas telefônicas, pelas instituições financeiras, pelos provedores de internet e pelas administradoras de cartão de crédito.

O ECA (Estatuto da Criança e do Adolescente) Lei 8.069/90 criou em seu estatuto o Art. 241-A que dispõem sobre o trafego na rede de dados de conteúdo sexual explicito ou pornográfico envolvendo criança ou adolescente. O Art 241-A, discorre:

> Art. 241-A Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático,

> fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente.

4.1 PROJETOS DE LEI

Persiste na sociedade a necessidade de aprimoramento da legislação vigente, onde o desenvolvimento do legislativo não consegue acompanhar a tamanha evolução tecnológica, ficando a sociedade a mercê de leis que não mais tão complexas e de tamanha abrangência quanto em relação ao ano em que entraram em vigor.

Assim como em todos os vetores da sociedade, em sentido estrito, o convívio humano na rede mundial de computadores sofre diuturnamente alterações, sobretudo em razão da criação de novos aplicativos, novos dispositivos e novas funções já existentes, daí o enquadramento das condutas perpetradas nestes meios perante a legislação já existente é desafio cotidiano das forças investigativas e do poder judiciário, por sua vez estes elementos constantemente se reportam ao legislativo para aprimoramento do conjunto normativo. (TOMASEVICIUS FILHO, 2016).

No ano de 2011 foi apresentado o projeto de Lei n 427, onde a fundamentação seria de incluir no Código Penal o crime de atentado quando se envolver o campo eletrônico ou de comunicações, mas segue aguardando relatório até o presente momento. (SENADO FEDERAL, 2012).

Já no âmbito do Senado Federal, aguarda deliberação o PLC nº 35 de 2012, já aprovado na Câmara dos Deputados, onde versa a acerca de tipificação criminal de vários delitos informáticos à serem incluídos no Código Penal. (SENADO FEDERAL, 2012)

Criada ao fim do ano de 2015 e colocada em pauta em abril de 2016, se tornou conhecida a CPI dos Crimes Cibernéticos, tendo como sugestões iniciais propostas que deveriam servir para complementar o Marco Civil da Internet, e ir

de encontro ao direito dos usuários da rede de computadores mais utilizada no mundo.

O documento que se tornou assunto da CPI trazia consigo diversas propostas de Projetos de Lei, e em maio de 2016 esse relatório teve aprovação integral por parte da Comissão Parlamentar.

Um dos PL's envolvidos no relatório, diz respeito a pirataria, e sobre a autonomia de um juiz determinar o bloqueio de um aplicativo de celular, sites, ou até mesmo uma rede social, caso seja considerado que estes estariam sendo utilizados para a pratica de crimes virtuais, e se tornou entre os demais o PL mais debatido entre os presentes, havendo polêmica na votação.

O fato que serviu de embate para esse PL se tornar polêmico, foi o fato de um Magistrado da Comarca de Sergipe ter decretado o bloqueio do aplicativo de mensagens WhatsApp, por 72 horas, onde gerou uma onda de comentários negativos entre os internautas, onde alegavam que o aplicativo deixou de ser simplesmente um aplicativo de conversas, mas se tornou uma ferramenta de trabalho para muitos, servindo de plataformas de vendas, suportes técnicos, e demais assuntos prioritários.

Não restando para os deputados a necessidade de se excluir do PL a possibilidade de um magistrado solicitar bloqueio de aplicativos de mensagens instantâneas de uso público, sendo mantido o restante do texto sem alterações.

Ainda, outra proposta pretende incluir os crimes praticados contra ou mediante computador, conectado ou não a rede, dispositivo de comunicação ou sistema informatizado ou de telecomunicação no rol das infrações de repercussão interestadual ou internacional que exigem repressão uniforme. (CÂMARA DOS DEPUTADOS, 2016).

Um dos projetos de leis mais atuais ainda em regime de tramitação, é o (PL 2514/2015) que tem como ementa a regular a forma, os prazos e os meios de preservação e de transferência de dados informáticos mantidos por

fornecedor de serviço a autoridades públicas, para fins de investigação criminal envolvendo delito contra criança ou adolescente, e dá outras providências. (CÂMARA LEGISLATIVA, 2016).

Juntamente com a Comissão de Segurança Pública e Combate ao Crime Organizado, foi levado a audiência pública na Câmara dos Deputados a matéria do PL 2514/2015, onde veio a contar com a participação de representantes do Ministério Público e Policia Federal.

Momento em que foi propicio ao MP solicitar que haja uma celeridade diante das empresas de telecomunicações quando forem notificadas a prestarem determinadas informações por determinação Judicial, principalmente quando houver teor de pedofilia, onde 1 (um) dia pode ser suficiente para se perder um dado e colocar toda uma investigação ao ponto de partida.

Todas as propostas legislativas aqui citadas, encontram-se em tramitação nas comissões temáticas, junto à outras inúmeras propostas de Projetos de Lei.

O Legislativo passa por dificuldades de aprovação de Leis devido a questões normais dos trâmites, e o vasto número de projetos de Lei na fila para análise.

CONCLUSÃO

O principal objetivo da presente monografia foi abordar a extrema relevância para a legislação brasileira em torno dos Crimes Virtuais, que se aceleram no processo de globalização, e abordar a respeito da inserção da tecnologia no campo cotidiano dos usuários.

Sabe-se que a sociedade se encontra em constante processo de evolução, e juntamente deveria acompanhar o legislativo, que regem as leis de todo o estado, para que sejam devidamente editadas e alteradas sempre que haver necessidade, para que somente assim se cumpra os direitos garantidos pela Constituição Federal.

É de notável conhecimento de todos que o Código Penal vigente se encontra em grande necessidade de reforma, afinal entrou em vigência em 1940, onde muitos crimes já se tornaram ineficientes e perdendo a relevância jurídica, enquanto novos crimes se espalham sem legislação regulamentadora.

Em suma, o aperfeiçoamento do Código Penal com penas mais severas, e um complexo de leis atualizadas, se tornaria mais positivas e melhor fundamentada, traria a função real do direito penal, que sempre foi a de versar sobre a proteção de bens jurídicos essenciais, promovendo essa proteção também no campo dos crimes virtuais.

Por fim, ressalta-se que bens jurídicos que são tutelados pelo Estado não podem permanecer sendo alanceados, devendo o Estado fazer se valer no papel de mantedor da ordem social, devendo possuir formas capazes de acompanhar todo crescimento evolutivo da internet, não permitindo que crimes cibernéticos permaneçam nas estatísticas de crimes sem a devida tipificação correta.

REFERÊNCIAS BIBLIOGRÁFICAS

JUS. **Globalização e Direito, uma analise a partir dos Direitos Humanos.** Disponível em: https://jus.com.br/artigos/53036/globalizacao-e-direito-uma-analise-a-partir-dos-direitos-humanos. Acesso em 18 Out 2020.

EM. **Noticia Nacional – Racker preso por roubar mais de 648 mil de contas bancárias.**
Disponível em: https://www.em.com.br/app/noticia/nacional/2020/08/24/interna_nacional,1178845/hacker-e-preso-por-roubar-mais-de-r-648-mil-de-contas-bancarias.shtml. Acesso em 12 de Ago de 2020.

AVG – **What is malware**
Disponível em: https://www.avg.com/pt/signal/what-is-malware. Acesso em 10 de Ago de 2020

TCA – **Blog Noticias – Como Denunciar um crime virtual passo a passo.**
Disponível em**:** https://www.tca.com.br/blog/como-denunciar-um-crime-virtual-passo-a-passo/. Acesso em 08 de Ago de 2020.

JUS BRASIL – **Artigos – Crimes Eletrônicos – LEI 12.737/2012**
Disponível em: https://godinhojradv.jusbrasil.com.br/artigos/405436426/crimes-eletronicos. Acesso em 14 de Ago de 2020.

JUS BRASIL – **Noticias – MP e PF pedem a provedores acesso mais rápido a dados sobre pedofilia.**
Disponível em: https://cd.jusbrasil.com.br/noticias/403739366/mp-e-pf-pedem-a-provedores-acesso-mais-rapido-a-dados-sobre-pedofilia. Acesso em 13 de Ago de 2020.

CAMARA LEG – **PL 2514/2015**
Disponível em:
https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=1594908. Acesso em 10 de Jul de 2020.

JUS BRASIL – **Noticias – CPI de crimes cibernéticos aprova relatório que atava liberdade na internet.**
Disponível em: https://csalignac.jusbrasil.com.br/noticias/339365280/cpi-de-crimes-ciberneticos-aprova-relatorio-que-ataca-liberdade-na-internet. Acesso em 10 de Jul de 2020.

JUS BRASIL – **Tópicos – Comissão Parlamentar de Inquérito do Crimes Cibernéticos.**
Disponível em: https://www.jusbrasil.com.br/topicos/91216792/comissao-parlamentar-de-inquerito-dos-crimes-ciberneticos. Acesso em 10 de Jul de 2020

JOTA **– Blog – Por 17 a 6 CPI dos Crimes Cibernéticos aprova relatório final**.

Disponível em: https://www.jota.info/paywall?redirect_to=//www.jota.info/justica/por-17-6-cpi-dos-crimes-ciberneticos-aprova-relatorio-final-04052016. Acesso em 09 de Jul de 2020.

CAMARA LEG – **Noticias – Relatório da CPI dos Crimes Cibernéticos sugere 19 medidas de combate aos delitos via internet.**
Disponível em: https://www.camara.leg.br/noticias/484426-relatorio-da-cpi-dos-crimes-ciberneticos-sugere-19-medidas-de-combate-aos-delitos-via-internet/. Acesso em 08 de Jul de 2020

JUS BRASIL – **Tópicos – Artigo 241 da Lei nº 8.069 de 13 de Julho de 1990.**
Disponível em: https://www.jusbrasil.com.br/topicos/10582366/artigo-241-da-lei-n-8069-de-13-de-julho-de-1990. Acesso em 08 de Jul de 2020

Planalto.gov – **Lei 12683/12**
Disponível em: http://www.planalto.gov.br/Ccivil_03/_Ato2011-2014/2012/Lei/L12683.htm#:~:text=Altera%20a%20Lei%20n%C2%BA%209.613,crimes%20de%20lavagem%20de%20dinheiro. Acesso em 16 de Jul de 2020

Segurança.uol – **Hackers e Crakers: quais as diferenças entre eles?**
Disponível em: https://seguranca.uol.com.br/antivirus/dicas/curiosidades/hackers_crackers_qual_a_diferenca_entre_eles.html#rmcl. Acesso em 13 de Jul de 2020

Julgado STJ – **Conflito de Competência nº 63.343-GO**

JUS BRASIL – **Lei 12965/14**
Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm#:~:text=Registros%20de%20Conex%C3%A3o-,Art.,ano%2C%20nos%20termos%20do%20regulamento. Acesso em 20 de Jul de 2020

Câmara - Leg – **Projeto para proibir crimes contra crianças e adolescentes gera opiniões.**
Disponível em: https://www.camara.leg.br/noticias/592722-projeto-para-coibir-crimes-ciberneticos-contra-criancas-e-adolescentes-divide-opinioes/ . Acesso em 12 de Out de 2020.

Emagis.com – **Definição de pornografia infantil: decisão do STJ**
Disponível em: https://www.emagis.com.br/area-gratuita/noticias/definicao-de-pornografia-infantil-nova-decisao-do-stj/. Acesso em 14 de Out de 2020.

Âmbito Juridico.com – **Dos crimes contra a honra**
Disponível em: https://ambitojuridico.com.br/cadernos/direito-penal/dos-crimes-contra-ahonra/#:~:text=Honra%20objetiva%20pode%20ser%20compreendida,inj%C3%BAria%20atinge%20%C3%A0%20honra%20subjetiva. Acesso em 10 de Out de 2020

Jus.com.br – **O direito a honra do individuo**
Disponível em: https://jus.com.br/artigos/54877/o-direito-a-honra-do-individuo-na-perspectiva-dos-danos-moral-e-material#:~:text=Isso%20%C3%A9%2C%20honra%20%C3%A9%20a,no%20sentimento%20da%20pr%C3%B3pria%20pessoa.&text=O%20direito%20a%20honra%20compreende,determinado%20indiv%C3%ADduo%20(honra%20objetiva). Acesso em 10 de Out de 2020

DireitoNet – **Dos Crimes contra a honra**
Disponível em: https://www.direitonet.com.br/artigos/exibir/9255/Dos-crimes-contra-a-honra. Acesso em 10 de Out de 2020.

Coalize.com – **Saiba tudo que pode levar à demissão por justa causa**
Disponível em: https://www.coalize.com.br/artigo-482-clt-demissao
Acesso em 05 de Ago de 2020

Jus.com.br – Espionagem eletrônica: resposta do governo americano e das empresas de tecnologia.
Disponível em: https://jus.com.br/artigos/25639/a-espionagem-eletronica-a-resposta-do-governo-americano-e-das-empresas-de-tecnologia
Acesso em 05 de Ago de 2020

Senado.Leg - **PLC 89/2003**
Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/63967**.** Acesso em 04 de Ago de 2020

Âmbito Jurídico **– Crimes Virtuais**: **elementos para uma reflexão sobre o problema na tipificação.**
Disponível em: https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-uma-reflexao-sobre-o-problema-na-tipificacao/
Acesso em 04 de Ago de 2020

Jesus, Damásio de. Manual **de Crimes Informáticos.** São Paulo: Saraiva, 2016.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011.

CUNHA, Rogério Sanches. **Manual de Direito Penal: Parte Geral.** Salvador: Juspodivm, 2014

SYDOW, Spencer Toth. **Delitos informáticos próprios: uma abordagem sob a perspectiva vitimodogmática.** 2009. Dissertação (Mestrado em Direito Penal) - Faculdade de Direito - Universidade de São Paulo, São Paulo, 2009. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/delitos_informaticos_proprios_uma_abordagem_sob_a_perspectiva_vitimodogmatica.pdf>. Acesso em: 12 de Jun de 2020.

TOMASEVICIUS FILHO, Eduardo. **Marco Civil da Internet: uma lei sem conteúdo normativo.** Estud. av., São Paulo , v. 30, n. 86, p. 269-285, Abr. 2016. Disponível em: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-40142016000100269&lng=en&nrm=iso. Acesso em 13 de Jun de 2020

SILVA, Jorge Vicente. **Estelionato e outras fraudes**. 1. ed. Curitiba: Juruá, 1995, p. 55.