UNICESUMAR - CENTRO UNIVERSITÁRIO DE MARINGÁ
CENTRO DE CIÊNCIAS HUMANAS E SOCIAIS APLICADAS
CURSO DE GRADUAÇÃO EM DIREITO

DOS CRIMES VIRTUAIS E AS CONSEQUÊNCIAS JURÍDICAS

GIOVANE OLIVEIRA DA SILVA

MARINGÁ – PR
2017

GIOVANE OLIVEIRA DA SILVA

DOS CRIMES VIRTUAIS E AS CONSEQUÊNCIAS JURÍDICAS

Artigo apresentado ao Curso de Graduação em Direito da UniCesumar – Centro Universitário de Maringá como requisito parcial para a obtenção do título de Bacharel em Direito, sob a orientação do Prof. Me. Lucas Yuzo Abe Tanaka.

MARINGÁ – PR

2017

FOLHA DE APROVAÇÃO

GIOVANE OLIVEIRA DA SILVA

DOS CRIMES VIRTUAIS E AS CONSEQUÊNCIAS JURÍDICAS

Artigo apresentado ao Curso de Graduação em Direito da UniCesumar – Centro Universitário de Maringá como requisito parcial para a obtenção do título de Bacharel em Direito, sob a orientação do Prof. Me. Lucas Yuzo Abe Tanaka.

Aprovado em: ____ de novembro de 2017.

BANCA EXAMINADORA

_____

Nome do professor – (Titulação, nome e Instituição)

_____

Nome do professor - (Titulação, nome e Instituição)

_____

Nome do professor - (Titulação, nome e Instituição)

DOS CRIMES VIRTUAIS E AS CONSEQUÊNCIAS JURÍDICAS

GIOVANE OLIVEIRA DA SILVA

RESUMO

Com o avanço da tecnologia, ampliaram-se os meios de comunicação entre as pessoas, afastando-as fisicamente tornando cada vez mais comum a comunicação virtual. Como advento e o acesso à rede mundial de computadores (internet) isso foi mais facilitado. O acesso ao ambiente virtual cada vez mais comum, em alguns países diminuiu certos crimes no meio social, sendo esses praticados através de um computador, conectado ou não a rede mundial de computadores. Embora existam benefícios, a internet tem trazido alguns problemas, devido a um acesso incorreto de informações dos seus usuários. O controle das condutas ilícitas é um tema que gera muitas discussões entre os especialistas no assunto, e que necessita de legislações mais específicas para controlar e combater tais crimes que acontecem no ambiente virtual. Da mesma forma, seus usuários devem seguir aos protocolos de proteção às suas informações, para protegê-las dos crimes virtuais que vem assolando o mundo moderno, e aparecem das mais diversas formas.

Palavras-chave: Internet. Direito. Ciberespaço.

VIRTUAL CRIMES AND THE LEGAL CONSEQUENCES

ABSTRACT

With the advancement of technology, the means of communication between people has been broadened, physically alienating them, making virtual communication more and more common. As advent and access to the world wide web (computers) this was made easier. Access to the increasingly common virtual environment in some countries has reduced certain crimes in the social environment, these being practiced through a computer, connected or not to the computer network. Although there are benefits, the internet has brought some problems due to incorrect access of information from its users. The control of illicit conduct is a topic that generates many discussions among experts in the subject, and requires more specific legislation to control and combat such crimes that occur in the virtual environment. Likewise, your users must follow the protocols protecting their information, to protect them from the virtual crimes that are plaguing the modern world, and they appear in many different ways.

Keywords: Internet. Right. Cyberspace.

1 INTRODUÇÃO

Desde o surgimento da humanidade, o homem é um ser social que necessita se comunicar um com o outro. Posto isso, o avanço da tecnologia proporciona maior praticidade e conforto às pessoas que a utiliza. E foi com este objetivo que o surgimento da internet não seria diferente, posto que a mesma é uma rede pública de computadores, que possibilita uma comunicação universal entre as pessoas que a ela estão conectados, não impondo fronteiras nem censura.

Porém, o avanço tecnológico também configurou um avanço de delitos e crimes diversos, em que se usa o meio virtual para a prática de ações desonestas, das mais variadas possíveis. Por isso, o Direito tem se voltado para conhecer e atualizar as leis, no que diz respeito à formas de proteção para os usuários da internet, conforme os casos específicos de crimes virtuais.

Dessa forma, o presente artigo tem por finalidade apresentar novos delitos e crimes que forma surgindo com o avanço da tecnologia, conhecendo alguns deles e demonstrando o quanto a legislação brasileira, embora esteja evoluindo, ainda está desamparada de leis específicas a serem aplicadas a esse tipo de crime, visto que as leis não tem conseguido acompanhar o avanço tecnológico.

Este tema é bastante atual, e traz à tona importantes discussões sobre o abuso da tecnologia, quando se trata de crimes virtuais, e que, com o passar do tempo, vem ocorrendo com cada vez mais frequência, sendo este um tema de suma importância neste momento, devendo a eles ser dada uma atenção especial.

Assim, após apresentarmos e analisarmos os conceitos e definições de internet, seus benefícios e crimes virtuais, apresentaremos alguns dos mais comuns tipos de crimes que acontecem na atualidade no ciberespaço, apontando as consequências jurídicas quando da prática desses crimes, bem como uma lei específica em vigor criada para combater vários crimes virtuais.

2 INTERNET: FERRAMENTA DE COMUNICAÇÃO ENTRE AS PESSOAS

2.1 CONCEITO DE INTERNET E ASPECTOS GERAIS

De maneira sucinta, podemos conceituar a Internet com a denominação utilizada por todos, que seria uma rede mundial de computadores. Nela há uma interligação entre pessoas, empresas e países, em que proporciona a viabilidade a todo tipo de informação possível, bastando ter um computador que tenha acesso a esse recurso. Atualmente, em qualquer lugar do mundo, é quase impossível não haver computadores ligados à rede.

Um dos conceitos apresentados sobre o que é internet, afirma que

> A rede de computadores consiste na ligação entre dois ou mais computadores e dispositivos (equipamentos) complementares acoplados através de recursos de comunicação, geograficamente distribuídos, permitindo a troca de dados entre estas unidades através de um sistema de comunicação e otimizando recursos de hardware e software. Este sistema de comunicação constitui-se de um arranjo topológico interligando os vários computadores (terminais – estações – nós) e de um conjunto de regras (protocolos), de forma a organizar a comunicação[1].

Conforme o trecho acima especifica, a internet é um meio de comunicação em nível global, proporcionando uma ligação entre os aparelhos conectados à rede, e que são protocolos de conexão específicos, conhecidos como TCP/IP, que traduzidos do inglês significam: Protocolo de Controle de Transmissão / Protocolo de Internet. Estes protocolos foram criados e desenvolvidos pela ARPA (Agência de Projetos de Pesquisa Avançada), sendo que tais protocolos estipulam as regras que têm que ser seguidas pelos computadores que se comunicam entre si ou com ou com outros computadores comunicados em outra rede.

Assim vejamos o principal dos protocolos de acesso à rede, o TCP/IP, que segundo Brandino é:

> Como existem diversos tipos de usuários e diversos tipos de aplicações, existem tecnologias de redes que se adequam melhor a cada perfil de usuário. O problema começa a surgir quando precisamos conectar diferentes tecnologias de redes de forma transparente. Torna-se então necessário um protocolo (ou linguagem) comum que independente da tecnologia de rede utilizada permita uma comunição (ou internetworking) de forma transparente. Neste contexto, o protocolo TCP/IP (Transport Control Protocol / Internet Protocol) vem suprir esta necessidade dando total transparência aos usuários finais das diversas tecnologias de rede empregadas pelas diversas LANs, MANs e WANs existentes, mascarando todos os detalhes da tecnologia de Hardware utilizada[2].

Assim como as pessoas físicas e jurídicas possuem um número de Cadastro de Pessoas Físicas e um número de Cadastro de Pessoas Jurídicas, respectivamente, com a finalidade de serem identificadas através destes, diferenciando-se uns dos outros, também na rede mundial

---

[1] MORAIS, Carlos Tadeu Queiroz de**. Conceitos sobre Internet e Web** – Porto Alegre: Editora da UFRGS, 2012, p. 13.

[2] BRANDINO, Wanderson Luiz. **Apostila TC/IP.** São Paulo: 1998, p. 4. Disponível em www.wandreson.com. Acesso em 18/10/2017.

de computadores, os computadores possuem seu próprio registro, sendo eles identificados através do seu endereço de IP, discutido acima, possibilitando que as atividades realizadas e desenvolvidas pelo computador sejam registradas e devidamente monitoradas.

2.2 ORIGEM HISTÓRICA E DEFINIÇÕES DA REDE MUNDIAL DE COMPUTADORES

A RMC – Rede Mundial de Computadores, conhecida mais especificamente como Internet, surgiu em Plena Guerra Fria, sendo esta considerada a "mãe" de todas as conexões, possibilitando o acesso virtual a todos os lugares do mundo.

Assim, a internet foi criada com objetivos militares, para que possibilitasse às forças-armadas dos EUA uma comunicação em caso de ataques impossibilitasse outros meios de comunicação. Nas décadas de 1970 e 1980 ela passou a ser utilizada também para uma comunicação acadêmica, onde professores e alunos universitários dos EUA poderiam se comunicar através dela[3].

Somente em 1990 que a internet alcançou a população em geral; ano em que o engenheiro inglês Tim Bernes-Lee desenvolveu a Worl Wide Web, possibilitando aos usuários a utilização de uma interface gráfica melhor e criação de sites mais dinâmicos (HISTÓRIA, 2017).

Antecessor à internet existia um projeto chamado ARPANET, de criação do Departamento de Defesa dos Estados Unidos que realizou uma interconexão de computadores, por meio de um sistema que era conhecido como comutação de pacotes, que era um esquema de transição de dados na rede de computadores, no qual as informações trocadas entre eles eram divididas em pequenos "pacotes", que continha trecho de dados, o endereço do destinatário, bem como informativo que possibilitava remontar a mensagem enviada originalmente (HISTÓRIA, 2010, p. 2).

Ao passar do tempo, várias redes já existentes aderiram a tecnologia desenvolvida pela ARPANET, passando a utilizá-la. O que possibilitou a existência da internet foi o Protocolo de Comunicação (*The Internet Protocol* – IP), permitindo então que qualquer computador, seja qual for a quantidade, fosse interligado em rede (GOUVEA, 1997).

A ARPANET e a INTERNET são redes cuja estrutura se dá de forma horizontal, não existindo hierarquia entre elas. Sendo assim, para que o acesso a elas seja liberado, basta um computador, uma linha telefônica e um modem.

---

[3] CASTELLS, Manuel. **A Galáxia da Internet.** São Paulo: Zahar (sem data), p. 3. Coleção Interfaces.

A história da internet é de tamanha complexidade que envolve vários aspectos tecnológicos e organizacionais e comunitários. Envolve quatro aspectos distintos, sendo eles:

a) evolução tecnológica por meio da qual começou as primeiras pesquisas sobre trocas de pacotes e a ARPANET; no qual os primeiros protocolos foram criados, para garantir o funcionamento de ambos.

b) aspectos operacionais e gerenciais de uma infraestrutura operacional complexa e global; diz respeito à possibilidade de um funcionamento em rede, atingindo todo mundo, de modo simultâneo e sem erros, no momento em que o usuário necessitar.

c) aspecto social que resultou numa larga comunidade de internautas trabalhando juntos para criar e evoluir com a tecnologia; envolve uma série de profissionais que buscaram, no desenvolvimento da internet, o seu aperfeiçoamento.

d) e aspecto de comercialização que resulta numa transição extremamente efetiva de pesquisa numa infraestrutura de informação disponível e utilizável (HISTÓRIA, 2010). Diz respeito à formas com que a internet possibilite também retorno financeiro, assegurando aos seus usuários o uso deste serviço com qualidade devida.

2.3 PONTOS POSITIVOS DA INTERNET

A internet mudou a forma de comunicação no mundo todo, estando cada vez mais presente em nossa vida, de maneira diária e corriqueira. A facilidade de comunicar-se com outras pessoas, seja lá onde estiver, possibilitando uma forma rápida e prática de comunicação é um dos principais pontos. Além deste, a ligação em rede possibilita efetuar compras on-line, visitar o mundo de maneira virtual, monitorar ambientes particulares, etc., de onde estiver da forma mais prática do mundo.

Dentre seus inúmeros pontos positivos, a internet possibilita, ainda, no desenvolvimento educacional, posto que esse recurso traz maneiras diversas de aprendizagem, permitindo a interação com pessoas do mundo inteiro, possibilitando a troca de informações, de conhecimento, cultural, entre outros. Possibilita ainda, com base na discussão e troca de informações, criar opiniões próprias, pensamentos críticos, e adquirir ainda mais personalidade.

A internet trouxe novas formas de comunicação, os comunicadores instantâneos como o MSN, Skype, Orkut, Facebook, entre outros, que são ferramentas baseados em internet, possibilitando uma verdadeira revolução na forma de comunicação entre as pessoas. Este é caracterizado como um ponto positivo, pelo fato de ter barateado o custo da comunicação,

assim como tornou as pessoas mais próximas, mesmo estando longe fisicamente umas das outras (MANCUZZO, 2014).

3 CRIMES VIRTUAIS

Juntamente com o surgimento da dos computadores, aparelhos eletrônicos, da internet e seus benefícios, surgiram crimes e criminosos especializados em cometer crimes no ciberespaço. Tais crimes possuem várias denominações, sendo chamados de crimes virtuais, crimes digitais, crimes transacionais, crimes por meio de informática, fraude informática, entre outros. Conforme cresce o número de conexões à rede de computadores, cresce também a criminalidade neste meio, sendo estes criminosos de certa forma "empurrados" pelo anonimato oferecido pelas dificuldades de investigação e identificação do autor do fato criminoso.

3.1 CONCEITO

Crimes virtuais são aqueles crimes praticados no ambiente virtual, ou seja, na internet, e que podem ser enquadrados no Código Penal Brasileiro; sendo o computador utilizado como um meio para a prática delitiva atingindo a própria vítima ou para atingir o computador do qual ela faz uso[4].

Augusto Rossini define o crime virtual como sendo:

> Conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade e a confidencialidade.[5]

A denominação de "crimes virtuais" para Augusto Rossini, refere-se a crimes e contravenções penais alcançando não somente as praticadas no âmbito da internet, mas sim levando em consideração qualquer conduta que esteja relacionada com o ambiente virtual,

---

[4] LIMA, Simão Prado. **Crimes Virtuais:** Uma Análise Da Eficácia Da Legislação Brasileira E O Desafio Do Direito Penal Na Atualidade. Disponível em <http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=15260&revista_caderno=3>. Acesso em: 18 de outubro de 2017.

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

seja ele de meio, ou de fim, abrangendo também delitos em que o computador seja utilizado como um instrumento para o crime a ser praticado.

Para Deborah Fisch Nigri, crime virtual é:

> Ato lesivo cometido por meio de um computador ou de um periférico com a intenção de se obter uma vantagem indevida. Segundo essa autora, os conceitos anglo-saxônicos limitam-se a denominar o direito de informática de *computer law* ou *legal aspects of computers* e, no caso mais específico de crimes informáticos, *computer crime*, isso porque o uso da palavra "informática" lhes é praticamente desconhecido.[6]

Como já mencionado anteriormente, acerca do que é propriamente crime, crime virtual, em outras palavras, é toda e qualquer ação típica, antijurídica e culpável cometida contra um computador conectado à rede mundial de computadores, sendo este usado como sendo o instrumento ou objeto do delito.

3.2 MODALIDADES

Muitas vezes o sistema informático é apenas um instrumento para a prática de um delito, e em alguns casos seria dispensável na realização da conduta antijurídica. Referimo-nos a delitos de ação livre, delitos esses que podem ser cometidos por inúmeros *modi operandi*. Por outro lado, há diversas condutas que somente poderiam ser praticadas contra o próprio sistema informático ou contra informações nele contidas.

3.2.1 Crimes Virtuais Próprios

Os Crimes virtuais Próprios são delitos cujos bens jurídicos atingidos são primordialmente os conhecidos como sistemas informatizados ou de telecomunicações ou dados.[7] Em outras palavras, estes são atos contra o computador e seu hardware (ou seja, contra o próprio material informático, que implica no computador propriamente dito e seus componentes eletrônicos), bem como seus atos contra dados ou programas de computador em geral.

Dessa forma, os chamados crimes virtuais próprios são aqueles que atingem o computador e seu sistema em geral. Neste caso, o computador é o alvo da prática delitiva,

---

[6] NIGRI, Deborah Fisch. **Crimes e segurança na Internet. In Verbis**, Rio de Janeiro: Instituto dos Magistrados do Brasil, ano 4, n. 20, p. 34, 2000.
[7] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011. p. 63.

havendo alguma forma de invasão, contaminação por vírus, destruição ou modificação de banco de dados, e que envolve questões como sabotagem do sistema, furto de propriedade intelectual, furto de informação, acesso abusivo, vandalismo cibernético, etc.

3.2.2 Crimes Virtuais Impróprios

Segundo Crespo (2011), crimes virtuais impróprios nada mais são do que aqueles já tradicionalmente tipificados em nosso ordenamento jurídico, mas que agora são praticados com auxílio de modernas tecnologias em geral. Portanto, essa denominação apenas representa que os ilícitos penais tradicionais podem ser cometidos por meio de novos *modi operandi*.

No entanto, estas formas são infrações já previstas penalmente, e que não são propriamente crimes de informática, ou seja, todos e quaisquer crimes que utilizarem a informática como instrumento para a sua execução, tendo o computador em geral como meio. Os chamados crimes virtuais impróprios são enquadrados, entre outros, contra o patrimônio e estelionato; contra a honra, calúnia; contra a liberdade individual, violação da intimidade, da correspondência e da liberdade de comunicação.

Dessa forma, o computador torna-se o instrumento para a prática delitiva, ocorrendo das mais diversas formas (fraude de conta bancária ou cartão de crédito, transferência de valores, divulgação ou exploração de pornografia, etc.).

3.3 CLASSIFICAÇÃO

Segundo Guimarães e Furlaneto Neto[8] os crimes virtuais podem ser classificados em puros, mistos e comuns, a saber:

a) crime virtual puro: compreende qualquer conduta que seja ilícita, a qual atenta o *hardware* e/ou *software* de um computador, ou seja, tanto a parte física quanto a parte virtual do microcomputador;

b) crime virtual misto: é aquele que utiliza a internet para a realização da conduta ilícita, e cujo objetivo se torna diferente do citado anteriormente. Por exemplo, as transações ilegais de valores de contas correntes;

---

[8] NETO, Mário Furlaneto; GUIMARÃES, José Augusto Chaves. **Crimes na internet:** elementos para uma reflexão sobre a ética informacional. Disponível em: <**http://www.cjf.jus.br/cf/revista/numero20/artigo9.pdf**>. Acesso em: 04 jul 2017.

c) crime virtual comum: é quando se utiliza a internet e seus meios virtuais apenas como forma de instrumento para realizar um delito que se enquadra no Código Penal, como por exemplo, distribuição de conteúdo pornográfico infantil por diversos meios, tais como *Messenger, e-mail, torrente* ou qualquer outra forma de compartilhamento de dados.

Há diversos termos que podemos utilizar para referirmos às atividades em que um computador é utilizado como uma ferramenta, meio de crime ou base de ataque, como: crime virtual, cibercrime, crime digital, crime eletrônico, crime informático, e-crime, etc.

Além da classificação anterior, podemos também caracterizar estes crimes, citados acima, em dois tipos: crimes cometidos onde o computador é utilizado como uma ferramenta cometer um delito e crimes cometidos contra o próprio computador, ou seja contra o computador em si, nos quais o objeto de certa forma é danificado ou prejudicado de alguma forma (GIMENES, 2013).

4 TIPOS DE CRIMES VIRTUAIS MAIS COMUNS

4.1 PORNOGRAFIA INFANTIL

Muitas pessoas se confundem, denominando de “pedofilia” os crimes de armazenamento e divulgação de imagens com conteúdo de pornografia infantil. Também é comum ocorrer de as pessoas chamarem a relação sexual entre uma pessoa maior de idade com uma pessoa menor de idade de “pedofilia”.

A lei brasileira pune diversas situações, envolvendo a exposição da sexualidade infantil em fotos, imagens, filmagens e interpretações teatrais[9], como por exemplo, a produção, reprodução filmagem e o registro de cenas de sexo explícito envolvendo crianças ou adolescentes.

No Brasil, o Estatuto da Criança e do Adolescente (Lei 8.069/90) define como sendo criança toda pessoa que possui 12 anos incompletos, e adolescente, toda pessoa com 12 anos completos e com até 18 anos incompletos.

No art. 240 da Lei 8.069/90, o referido Estatuto da Criança e do Adolescente estão os principais crimes que envolvem pornografia infantil, bem como a pena que é aplicada ao infrator:

---

[9] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011. p. 90.

> Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente:
> Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.
> § 1º Incorre nas mesmas penas quem agencia, facilita, recruta, coage, ou de qualquer modo intermedeia a participação de criança ou adolescente nas cenas referidas no caput deste artigo, ou ainda quem com esses contracena.
> § 2º Aumenta-se a pena de 1/3 (um terço) se o agente comete o crime:
> I – no exercício de cargo ou função pública ou a pretexto de exercê-la;
> II – prevalecendo-se de relações domésticas, de coabitação ou de hospitalidade; ou
> III – prevalecendo-se de relações de parentesco consanguíneo ou afim até o terceiro grau, ou por adoção, de tutor, curador, preceptor, empregador da vítima ou de quem, a qualquer outro título, tenha autoridade sobre ela, ou com seu consentimento.

4.2 ESTELIONATO

O estelionato é uma prática criminosa, em que um individuo obtém vantagem de forma ilícita em cima de outro. Ele ocorre, por exemplo, quando uma pessoa vende, cede ou hipoteca algo para mais de uma pessoa, enganando-a ou enganando a um grupo determinado.

Assim dispõe o Código Penal (Lei 2.848/90), em seu art. 171, sobre o estelionato, bem como a pena que é aplicada ao infrator:

> Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:
> Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis.
> § 1º - Se o criminoso é primário, e é de pequeno valor o prejuízo, o juiz pode aplicar a pena conforme o disposto no art. 155, § 2º.
> [...]

O estelionato é consumado quando há o alcance da vantagem ilícita, havendo prejuízo alheio, frisando-se a última parte, que é necessário haver o prejuízo alheio.

Uma das práticas mais comuns que temos de estelionato hoje em dia são as de absurda redução de preços de mercadorias em sites de vendas de produtos pela internet, através da clonagem de sites, não havendo então a entrega do produto após o pagamento pelo cliente.

4.3 *REVENGE PORN*

O *Revenge Porn*, palavra inglesa que traduzida para o português significa “pornografia de vingança”, é o ato de expor na internet fotos e/ou vídeos íntimos de terceiros sem o consentimento destes, geralmente contendo cenas de sexo explícito que mesmo quando gravadas de forma consentida, não tinham a intenção de divulgá-las publicamente pelas partes

que gravaram. No entanto, após o fim do relacionamento, uma das partes divulga as cenas íntimas na internet como forma de "vingar-se" da pessoa com quem se relacionou. Em muitos desses casos, os autores e cúmplices sequer conhecem a vítima e mesmo assim, divulgam o conteúdo por mera diversão.

No tocante à legislação, no Brasil não existe ainda uma lei específica para este tipo de caso; no entanto, isso depende de uma análise real dos fatos acontecidos, para que seja aplicada uma pena. Usualmente, tais condutas são tipificadas como injúria ou difamação. Nos casos em que a vítima é menor de idade, aplicamos o disposto no ECA – Lei 8.069/90, em que a pena é de reclusão de 03 a 06 anos (CUNHA, 2017).

4.4 CRIMES CONTRA A HONRA

Os crimes contra a honra são aqueles que estão previstos nos arts. 138 a 140 do Código Penal (Lei 2.848/90), e são uns dos mais comuns praticados no ambiente da internet.

A Honra está ligada a qualidades físicas, intelectuais e morais de uma pessoa, e que faz com que a pessoa seja respeitada no âmbito social, dizendo respeito, ainda, à sua autoestima. A honra revê o valor social da pessoa, de modo que leva à aceitação ou rejeição da pessoa à sociedade.

O que motiva os criminosos à prática destes crimes é o anonimato que lhes são “oferecidos”, e tais crimes podem ocorrer nas redes sociais, pelo envio de *spams*, em blogs, chats, etc.

4.4.1 Calúnia

É a atribuição de um fato criminoso a alguém, sabendo o autor de que é falsa tal acusação. É preciso que se atribua a um sujeito passivo certo um fato antijurídico previsto em lei e que tal atribuição se faça sabendo que é mentirosa.

Caso o agente esteja de boa fé, supondo erroneamente ser verdadeira, a intenção estará excluída, excluindo-se também o crime.[10] Porém, quando há má fé, o agente pode ser indiciado.

São exemplos de calúnia: espalhar e-mails, dizer em aplicativos de conversa ou publicar nas redes sociais que certa pessoa abusou sexualmente de outra ou que roubou

[10] Ibid., p. 90

dinheiro da empresa em que trabalha, entre outros, sendo estes os mais comuns tipos que decorrem na Lei.

Aos crimes de calúnia, conforme art. 138 do Código Penal, a pena é de detenção e varia de 06 meses a 02 anos.

4.4.2 Difamação

Nos crimes de difamação é atribuído à pessoa um fato específico, mas que não seja considerado crime, pois, senão, seria considerado crime de calúnia e não de difamação. Neste caso, ofende a reputação da pessoa. A lei não exige a atribuição falsa de fato desonroso, como na calúnia, pois mesmo que seja verdadeiro o fato, configura-se crime de difamação.

A difamação, assim como a calúnia, é consumada quando a terceira pessoa toma conhecimento do fato ofensivo à honra da vítima, mesmo que ela ainda não tenha tido conhecimento do fato.

São exemplos de difamação: enviar e-mails ou publicar nas redes sociais que determinada pessoa está se drogando ou se prostituindo diariamente.

Aos crimes de difamação, conforme art. 139 do Código Penal, a pena é de detenção e varia de 03 meses a 01 ano.

4.4.3 Injúria

No crime de injúria, há a violação da honra subjetiva da pessoa. Consiste em injuriar alguém, ofendendo a dignidade ou o decoro. Enquanto a dignidade compreende os valores morais que compõem a personalidade, o decoro abarca as qualidades de ordem física e intelectual.[11]

Injuriar é ofender, falar mal, insultar, sem necessidade de atribuir a alguém um fato determinado[12], ou seja há atribuições de características negativas a pessoa, sobre suas qualidades físicas, intelectuais, morais.

São exemplos de injúria: enviar e-mails ou publicar nas redes sociais que tal pessoa é gora, magrela, vaca, retardada, etc., ou seja, comentar sobre características negativas de uma pessoa.

---

[11] PRADO, Luiz Regis. **Comentários ao código penal**. 8. ed. rev., atual. rev. e ampl. São Paulo: Revista dos Tribunais, 2013.p. 493.

[12] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011. p. 91.

Aos crimes de difamação, conforme art. 139 do Código Penal, a pena é de detenção e varia de 01 a 06 meses.

5 LEI CAROLINA DIECKMANN – LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012

A lei dispõe sobre a tipificação criminal de delitos cometidos no mundo virtual, ou seja, na Rede Mundial de Computadores, e recebeu o apelido de "Lei Carolina Dieckmann" devido a sua aprovação ter sido estimulada depois de a atriz ter fotos íntimas vazadas na internet em maio de 2012.

Em meados de abril de 2012, *hackers* enviaram um *malware* para o e-mail da atriz, que acabou clicando no arquivo, e abri-lo liberou uma porta para a instalação de um programa, permitindo então aos *hackers* o acesso ao computador da atriz. Com isso, 60 arquivos foram copiados do computador dela, entre eles, as fotos íntimas publicadas na internet. Antes da publicação das fotos, houve uma tentativa de extorsão por parte dos *hackers*, pendendo à atriz uma quantia de R$ 10.000,00 (dez mil reais) para que não divulgassem as fotos. A atriz não cedeu à chantagem e então teve suas fotos publicadas em sites pornográficos.[13]

A referida lei foi introduzida no Código Penal Brasileiro, sendo parte no Art. 154-A, conforme abaixo:

> 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.
> § 1º 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.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º 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.
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:

[13] YOUTUBE, 2012.

> 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.

Mesmo essa lei ter sido criada para punir delitos assegurando assim, a segurança digital no país, ela tem recebido diversas críticas de especialistas na área, por diversos fatores, dentre eles, a forma com que as punições são impostas.

Invadir dispositivo informático, tais como smartphones, tablets, computadores, entre outros, foi tipificado como crime por uma legislação específica, além de ter sido incluído junto a ela, a interrupção de serviços informáticos de utilidade pública também tipificada como crime, abrangendo ainda, cartões de crédito/débito como documentos pessoais, tornando sua falsificação como crime.

De acordo com o *caput* do artigo, o objetivo de tipificar a invasão do dispositivo eletrônico, visa à proteção da privacidade e intimidade da pessoa, bem como as informações do proprietário do dispositivo. De outro lado, a lei deixa claro que a invasão deve ter como objetivo o acesso aos dados visando a alteração ou destruição deles, que no caso a pessoa mantinham preservados. Além disso, o proprietário do dispositivo eletrônico deve impor alguma medida de proteção de tais dados, demonstrando claramente que não deveriam aqueles dados ser de conhecimento público, bem como não deve autorizar o aceso ao dispositivo invadido.

Outro ponto bastante criticado é o fato de a lei tipificar a infração dentro de três critérios, sendo eles: 1) invasão do dispositivo; 2) mediante violação do mecanismo de segurança; e 3) para adulterar ou destruir dados com a obtenção de vantagens ilícitas. Neste sentido, se uma pessoa invadir um equipamento, mas não subtrair ou copiar nada, não haverá a caracterização de crime, ou seja, se não haver nenhuma dessas condicionantes, provavelmente, o ilícito vai se caracterizar apenas na esfera cível.

De acordo com a lei, quem produz ou difunde dispositivos ou programas de computador, como vírus, também é enquadrado pela nova lei, porém, a clonagem de redes, por exemplo, não está definida na norma.

Conforme a nova legislação, os crimes virtuais poderão ser punidos com pena de multa mais detenção, variando de 06 meses a 02 anos, podendo ser elevada em alguns casos específicos. As punições poderiam/deviam ser maiores, evitando que os criminosos tivessem o “benefício” do juizado especial criminal. Neste juizado, atendendo a alguns requisitos, tais

como, não ter sido condenado anteriormente, ou não ter sido julgado por este juizado num período de 05 anos, e a pena não ultrapassando 02 anos, o réu tem direito de ao invés de cumprir pena, pagar cestas básicas ou prestar serviços à comunidade, por exemplo. Mesmo assim, a lei, de certa forma, demonstra um avanço do legislador, podendo ela ser aplicada na maioria dos casos.

Como as vítimas não podem também ficarem totalmente desamparadas pelo fato de não terem habilitado senha no dispositivo, há diversos mecanismos de segurança, que através de perícia, podem ser utilizados como comprovação do delito, a exemplo do *firewall* do Windows.

Para melhor se proteger, as pessoas devem criptografar arquivos ou pastas do computador que não pretendem que seja de conhecimento de outras pessoas, bem como realizar backups com frequência em dispositivos móveis, como HD externo, pen drive, etc.

6 CONSIDERAÇÕES FINAIS

Claramente, os crimes virtuais são comuns hoje em dia, assim como crimes cometidos fora da internet. Isso se dá pela prática que as pessoas têm de se comunicarem virtualmente, e pelo avanço de tecnologias que podem ser tanto usadas para o bem, como para o mal. O que ocorre na atualidade é que grande parte dos crimes que no passado aconteciam no “mundo concreto”, hoje acontecem no mudo virtual e por isso, precisam de leis que acompanhem essa tendência. Houve então uma transição da forma com que eles são praticados.

Com isso, a legislação tem tido mudanças, e deve acompanhar a tecnologia utilizada, sendo por isso, criadas novas leis para que os criminosos sejam punidos pela prática dos crimes, como também devem estas leis ser atualizadas e adequadas para facilitar a identificação do autor que cometeu um delito, bem como para facilitar a aplicação da punição.

A criação de novas leis não deve ser feita como no caso da Lei Carolina Dieckmann, criada às pressas. Sendo assim, muito específica a um caso, que na verdade não se aplicaria a referida lei ao caso que deu motivo a sua aceleração e criação. Por isso, devem ser menos específicas, mais amplas e menos complexas, para que possam ser enquadrados vários tipos penais em apenas uma lei.

Por fim, notamos o quanto somos carentes de leis que versam sobre crimes virtuais e o quanto necessitamos da criação de novas leis para enquadrarmos vários tipos penais que surgem com o avanço tecnológico. Sabemos que é praticamente impossível acabar com a

criminalidade, mas que temos que tentar combater ao máximo possível esse problema, que está se tornando de cunho social.

REFERÊNCIAS

BRANDINO, Wanderson Luiz. **Apostila TC/IP.** São Paulo: 1998, p. 4. Disponível em <www.wandreson.com>. Acesso em 18/10/2017.

BRASIL. **Código Penal Brasileiro**. Decreto-lei n. 2.848/40. Brasília: Senado Federal, 1940.

_____. **Estatuto da Criança e do Adolescente**. Lei 8.069/90. Brasília: Senado Federal, 1990.

_____. **Juizados Especiais Cíveis e Criminais**. Lei 9.099/95. Brasília: Senado Federal, 1995.

CASTELLS, Manuel. **A Galáxia da Internet.** São Paulo: Zahar (sem data), p. 3. Coleção Interfaces.

COLLI, Maciel. **Cibercrimes:** limites e perspectivas à investigação policial de crimes cibernéticos. Curitiba: Juruá, 2010.

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

CUNHA, Lia Calegari da. ***Revenge Porn* e seus aspectos jurídicos**. Disponível em: <https://jota.info/artigos/revenge-porn-e-seus-aspectos-juridicos-18032017>. Acesso em 13 jul. 2017.

GIMENES, Emanuel Alberto Sperandio Garcia. **Crimes Virtuais**. Revista de Doutrina da 4ª Região, Porto Alegre, n. 55, ago. 2013. Disponível em: <http://www.revistadoutrina.trf4.jus.br/index.htm?http://www.revistadoutrina.trf4.jus.br/artigos/edicao055/Emanuel_Gimenes.html>. Acesso em: 23 jun. 2017.

GOUVEIA, Sandra Medeiros Proença. **O direito na era digital**: Crimes praticados por meio da informática. Rio de Janeiro: Mauad, 1997. Disponível em: <http://books.google.com.br/books?id=3vzmW3DtAuQC&pg=PA43&lpg=PA43&dq=o+legislador+come%C3%A7ou+a+se+preocupar+com+o+mau+uso+dos+recursos+da+inform%C3%A1tica&source=bl&ots=TDsESpVdyx&sig=HFP7BDOai9J5BzdZjtElpc0SU8&hl=ptBR#v=onepage&q=o%20legislador%20come%C3%A7ou%20a%20se%20preocupar%20com%20o

%20mau%20uso%20dos%20recursos%20da%20inform%C3%A1tica&f=false>. Acesso em: jun. 2012.

HISTÓRIA. **História da internet**. Disponível em: <http://www.suapesquisa.com/internet>. Acesso em: 19 jun. 2017.

HISTÓRIA. **História da internet**. Disponível em: <http://www.slideshare.net/guest06f3c/historia-da-internet-1162354>. Acesso em: 19 jun. 2017.

LIMA, Simão Prado. **Crimes Virtuais:** Uma Análise Da Eficácia Da Legislação Brasileira E O Desafio Do Direito Penal Na Atualidade. Disponível em <http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=15260&revista_caderno=3>. Acesso em: 18 de outubro de 2017.

MANCUZZO, Fabiano, **Importância da internet na sociedade**, DNBR Telecom, 2014. Disponível em: <http://www.dnbr.com.br/2014/11/importancia-da-internet-na-sociedade/>. Acesso em: 20 jun. 2017.

MORAIS, Carlos Tadeu Queiroz de**. Conceitos sobre Internet e Web** – Porto Alegre: Editora da UFRGS, 2012, p. 13.

NETO, Mário Furlaneto; GUIMARÃES, José Augusto Chaves. **Crimes na internet:** elementos para uma reflexão sobre a ética informacional. Disponível em: <http://www.cjf.jus.br/cf/revista/numero20/artigo9.pdf>. Acesso em: 04 jul. 2017.

NOGUEIRA, Duda. **Pornografia de Vingança (*Revenge Porn*) Por Gracielle Torres**. Latinoware. Foz do Iguaçú, 2015. Disponível em: <http://latinoware.org/pornografia-de-vinganca-ou-revenge-porn/>. Acesso em: 13 jul. 2017.

OLIVEIRA, Luiz Gustavo Caratti de; DANI, Marília Gabriela Silva. **Os crimes virtuais e a impunidade real**. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=9963>. Acesso em: 05 ago. 2017.

PINHEIRO, Emeline Piva. **Crimes virtuais: uma análise da criminalidade informática e da resposta estatal**. 2011. 34f. Artigo (Graduação em Direito) – Universidade Federal de Santa Catarina, Florianópolis, 2011.

PINHEIRO, Patrícia Peck. **Direito digital**. 4. ed. rev., atual. e ampl. São Paulo: Saraiva, 2010.

Polícia Encontra Hackers Que Roubaram Fotos De Carolina Dieckmann Pelada – Fantástico. Youtube, 2012. Duração: 08MIN24SEG. Disponível em: <https://www.youtube.com/watch?v=homxwmsdcow>. ACESSO EM: 29 JUL. 2017.

PRADO, Luiz Regis. **Comentários ao código penal**. 8. ed. rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2013.

_____; CARVALHO, Érika Mendes de; CARVALHO, Gisele Mendes de. **Curso de direito penal**. 13. ed. rev., atual. e ampl. São Paulo: Revista dos Tribunais, 2014.