MAURILEIDE DA SILVA SOARES

CRIMINALIDADES EMERGENTES APARTIR DAS NOVAS TECNOLOGIAS DE INFORMAÇÕES & COMUNICAÇÃO NO DIREITO PENAL

FACULDADE FASIPE / CPA
CUIABÁ
2022

MAURILEIDE DA SILVA SOARES

CRIMINALIDADES EMERGENTES APARTIR DAS NOVAS TECNOLOGIAS DE INFORMAÇÕES & COMUNICAÇÃO NO DIREITO PENAL

Trabalho de Conclusão de Curso apresentado à Banca Avaliadora do Departamento de Direito, da Faculdade de Cuiabá/CPA - FASIPE, como requisito parcial para a obtenção do título de Bacharel em Direito.

Orientador (a): Prefº. Ronildo Medeiros Junior

FACULDADE FASIPE / CPA
CUIABÁ
2022

Maurileide Silva Soares

CRIMINALIDADES EMERGENTES APARTIR DAS NOVAS TECNOLOGIAS DE INFORMAÇÕES & COMUNICAÇÃO NO DIREITO PENAL

Trabalho de Conclusão de Curso apresentado à Banca Avaliadora do Curso de Direito - FASIPE, Faculdade de Cuiabá/CPA como requisito parcial para a obtenção do título de Bacharel em Direito.

Aprovado em 22 de agosto de 2022

_____

Ronildo Medeiros Junior
Professor (a). Orientador (a)
Departamento de Direito –FASIPE

_____

Diego Castro de Mello
Professor (a). Avaliador (a)
Departamento de Direito –FASIPE

_____

Ronildo Medeiros Junior
Coordenador do Curso de Direito
FASIPE - Faculdade de Cuiabá/CPA

FACULDADE FASIPE / CPA
CUIABÁ
2022

DEDICATÓRIA

Dedico a Deus por nunca ter desistido de mim.

AGRADECIMENTOS

- A Deus em primeiro lugar!

- A minha família, que foi fundamental nessa jornada. Aos meus Filhos e em especial ao meu esposo Mario Paulo dos Santos Filho que não me deixou desistir e foi alicerce durante todo o Curso.

-Ao meu orientador o professor Ronildo Medeiros Junior pelas orientações e paciência.

-Ao meu Sobrinho Diego Cruz, advogado e inspiração para escolha deste curso, provedor e mentor, o qual proporcionou esta oportunidade

-Aos nobres professores pelos conhecimentos técnicos, científicos transmitidos na pratica.

-E todas as pessoas que de alguma forma contribuíram direta ou indiretamente para a elaboração deste trabalho.

-E por fim, a minha pessoa por nunca ter desistido desta realização.

RESUMO

O atual trabalho demonstra o posicionamento da pesquisa em relação a fragilidade do ordenamento Jurídico Brasileiro aos crimes cibernéticos, diante do grande avanço da tecnologia da internet. A metodologia aplicada a este trabalho visa explorar os campos de conflitos, dentro das diversidades encontradas nos crimes cibernéticos e suas leis, analogia, decretos, condutas dos criminosos assim como também a tipificação dos crimes. Demonstra de forma simples os mecanismos tecnológicos que regem no campo da internet criados para contribuir com a humanidade, porém são usados para efetuar tais crimes. As leis estão presente de forma clara e objetivas afim de elucidar ou iluminar quaisquer dúvidas sobre este tema tão controverso. Abordamos assuntos que a própria jurisprudência aqui apresentada serve como meio de consulta para buscar um direcionamento mais amplo sobre as leis que regem os crimes cibernéticos, sabendo da carência legislativa de uma lei especifica em nosso País em relação a este assunto tão importante no campo jurídico dentro da Legislação Brasileira.

Palavras-chave: Crimes Cibernéticos; Legislação Brasileira; Jurisprudência; Código Penal; Legislação Específica.

ABSTRACT

The current work demonstrates the position of the research in relation to the fragility of the Brazilian legal system to cyber crimes, in the face of the great advance of internet technology. The methodology applied to this work aims to explore the fields of conflicts, within the diversities found in cyber crimes and their laws, analogy, decrees, criminal conduct as well as the typification of crimes. It demonstrates in a simple way the technological mechanisms that govern the field of the internet created to contribute to humanity, but are used to carry out such crimes. The laws are present in a clear and objective way in order to elucidate or clarify any doubts about this controversial topic. We address issues that the jurisprudence presented here serves as a means of consultation to seek a broader direction on the laws that govern cyber crimes, knowing the legislative lack of a specific law in our country in relation to this very important subject in the legal field within of Brazilian Legislation.

Keywords: Cyber Crimes; Brazilian legislation; Jurisprudence; Penal Code; Specific Legislation.

SUMÁRIO

CAPITULO 4 – JURISPRUDÊNCIA

APRESENTAÇÃO

O advento da internet trouxe ao mundo enorme transformação nas mais diversas relações sociais, em razão desse grande avanço da tecnologia, novos tipos de crimes começaram a surgir dentro do meio virtual, sendo esses denominados de ciber crimes.

O resultado crescente dessas novas modalidades resultou no crescimento do debate jurídico acerca desse novo contexto. Sendo assim, o presente trabalho objetiva a discussão sobre os crimes cibernéticos e a maneira na qual a legislação brasileira se relaciona com tal tema.

INTRODUÇÃO

O mundo moderno sofreu diversas mudanças com o passar do tempo, dentre elas, o uso da internet se tornou indispensável para viver em sociedade e, atualmente, tal ferramenta diária é a mais utilizada pelas pessoas. Em consequência disso, a criminalidade se adaptou às novas possibilidades humanas e, a fito de cometer ilegalidades, elaborou mecanismos novos para a realização de crimes no meio digital, como também, com o desenvolvimento da legislação brasileira, urge a discussão acerca das jurisprudências diante dos novos contextos emergentes, cuja a finalidade de impedir o crescimento dessas novas práticas opera dentro da realidade penal brasileira.

A internet impactou todo o corpo social e, com a revolução da internet, a sociedade teve que se adaptar na mesma velocidade em que a tecnologia avançava e se tornava cada vez mais presente na vida dos indivíduos, consequentemente, foram criados novos crimes e, a partir desses, foi salientada a necessidade de desenvolver e criar leis e normas para punir de forma efetiva os ciber criminosos.

No entanto, a cada dia que passa são criados novos mecanismos, programas, máquinas e objetos tecnológicos, tornando o crescimento desenfreado oportunizando para o cibe crime. Nesse sentido, a internet se faz essencial e, como tudo que se renova, gera um novo ordenamento jurídico brasileiro, o qual busca incansavelmente criar leis para punir os crimes cibernéticos, esses que ferem constitucionalmente os direitos das pessoas, empresas e organizações, como também, fere de forma brutal a dignidade humana. Com isso, aborda-se neste trabalho as legislações que punem e delimitam o crime cibernético.

Ao cabo, tal trabalho atua sob a premissa de contribuir para com o cenário penal inserido, propiciando e esclarecendo, por meios acadêmicos e científicos, o certame dos crimes virtuais, pois se trata de um tema pouco debatido e aprofundado, tanto dentro do meio social quanto dentro do meio jurídico.

CAPITULO 1 - CRIMES CIBERNETICOS

No primeiro momento vamos abordar a classificação e os conceitos preliminares que estão presentes nos crimes cibernéticos.

A internet é, sem dúvidas, a maior revolução tecnológica do último século. Porem também se tornou uma ferramenta para criminosos. As novas tecnologias de informação surgem trazendo mudanças ao contexto social ao redor do mundo. A fragilidade em guardar as suas informações e dados diante de uma comunicação virtual crescente entre as pessoas se acentua de uma forma jamais vista, o que, de maneira negativa, contribui para o crescimento dos ciber crimes na medida em que cria novas oportunidades.

1.1 Conceito e Classificação dos Crimes Cibernéticos

Na falta de um conceito mais amplo e direto sobre o crime cibernéticos fica difícil contextualizar juridicamente ou até mesmo buscar uma bibliografia a respeito do assunto do que seja crime cibernético. Fica aqui exposta a definição do Jurista e Professor Damásio de Jesus, que, de forma pratica, demonstra:

> Conceituamos crime informático como o fato típico e antijurídico cometido por meio da ou contra a tecnologia da informação. Decorre, pois, do Direito informático, que é o conjunto de princípios, normas e entendimentos jurídicos oriundos da atividade informática. Assim, é um ato típico e antijurídico, cometido através da informática em geral, ou contra um sistema, dispositivo informático ou rede de computadores. Em verdade, pode-se afirmar que, no crime informático, a informática ou é o em ofendido ou o meio para a ofensa a bens já protegidos pelo Direito Penal. (JESUS, Damásio de, 2016, p. 49).

Os crimes cibernéticos são os mesmos, a maioria já existentes, delitos e infrações. Mas o que mudou? Foi a fragilidade com que a internet contribui para aumentar a acessibilidade aos dados e informações que muitas das vezes são restritas e mesmo protegidas.

Podemos classificar os crimes cibernéticos diante de uma referência bibliográfica como crimes próprios e impróprios conforme Spencer Toth Sydow (2015 p.88):

> Delitos informáticos impróprios são delitos comuns, portanto condutas típicas, antijurídicas e culpáveis, que são perpetradas utilizando-se de mecanismos informáticos como ferramental, sendo que outros meios poderiam ter sido igualmente eleitos para a pratica. São, pois, delitos de forma livre. Por sua vez, delitos informáticos próprios são as condutas típicas antijurídicas e culpáveis que visam atingir um sistema informático ou seus dados, precisamente violando sua confidencialidade, sua integridade ou sua disponibilidade. São delitos de forma vinculada.

Em concordância das classificações de crimes cibernéticos o Jurista Damásio de Jesus (2016, p. 52-53) apresenta a classificação dos crimes como sendo mediato ou indireto, citado abaixo:

> Assim, classificamos os crimes informáticos em:
>
> a) crimes informáticos próprios: em que o bem jurídico ofendido é a tecnologia da informação em si. Para estes delitos, a legislação penal era lacunosa, sendo que, diante do princípio da reserva penal, muitas práticas não poderiam ser enquadradas criminalmente;
>
> b) crimes informáticos impróprios: em que a tecnologia da informação é o meio utilizado para agressão a bens jurídicos já protegidos pelo código Penal brasileiro. Para estes delitos, a legislação criminal é suficiente, pois grande parte das condutas realizadas encontra correspondência em algum dos tipos penais;
>
> c) crimes informáticos mistos: são crimes complexos em que, além da proteção do bem jurídico informático (inviolabilidade dos dados), a legislação protege outro em jurídico. Ocorre a existência de dois tipos penais distintos, cada qual protegendo um bem jurídico;
> d) crime informático mediato ou indireto: trata-se do delito informático praticado para a ocorrência de um delito não informático consumado ao final. Em Direito informático, comumente um delito informático é cometido como meio para a prática de um delito-fim de ordem patrimonial. Como, por exemplo, no caso do agente que captura dados bancários e usa para desfalcar a conta corrente da vítima. Pelo princípio da consunção, o agente só ser punido pelo delito-fim (furto). (JESUS, Damásio de, 2016, p. 52,53).

Sabendo que os conceitos bibliográficos que aqui abordamos podem sofrer alterações conforme o desenvolvimento dos conceitos jurídicos, mostrando em um pouco espaço de tempo uma nova visão sobre os crimes cibernéticos.

1.2 Dispositivo Informático

A tipificação do Crime mante-se no art. 154-A do Código penal, apresentado a seguir:

> Invasão de dispositivo informático (Incluído pela Lei nº 12.737, de 2012) Vigência
>
> 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: (Incluído pela Lei nº 12.737, de 2012) Vigência
>
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. (Incluído pela Lei nº 12.737, de 2012) Vigência
>
> §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. (Incluído pela Lei nº 12.737, de 2012) Vigência
>
> §2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico. (Incluído pela Lei nº 12.737, de 2012) Vigência
>
> §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: (Incluído pela Lei nº 12.737, de 2012) Vigência
>
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave. (Incluído pela Lei nº 12.737, de 2012) Vigência
>
> §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 obtidas. (Incluído pela Lei nº 12.737, de 2012) Vigência
>
> §5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
>
> (Incluído pela Lei nº 12.737, de 2012) Vigência
>
> I - Presidente da República, governadores e prefeitos; (Incluído pela Lei nº 12.737, de 2012) Vigência
> II - Presidente do Supremo Tribunal Federal; (Incluído pela Lei nº 12.737, de 2012) Vigência
> 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 (Incluído pela Lei nº 12.737, de 2012) Vigência
> IV - Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (Incluído pela Lei nº 12.737, de 2012) Vigência

Foi retratado um crime conforme o adveio da Lei 12.737/2012 para preencher um vácuo normativo no caso da atriz Carolina Dieckmann Worcman pelos crimes de extorsão, difamação e furto.

Segundo Guilherme de Souza Nucci: “Invadir significa violar, transgredir, entrar força em algum lugar, carregando o verbo nuclear do tipo um forte conteúdo normativo. ”

Conforme Rogério Sanches Cunha (2017 p. 264), o dispositivo informático se refere:

> Por dispositivo informático entende-se qualquer aparelho (instrumento eletrônico) com capacidade de armazenar e processar automaticamente informações/programas (Notebook, Netbook, Tablet, Ipad, Iphone, Smartphone, pendrive etc.)

Segundo Cléber Masson (2018, p. 330), os dispositivos informáticos têm quatro grupos:

> Os dispositivos informáticos dividem-se basicamente em 4 (quatro) grupos: dispositivos de processamento: são responsáveis pela análise de dados, com o fornecimento de informações, visando a compreensão de uma informação do dispositivo de entrada para envio aos dispositivos de saída ou de armazenamento. Exemplos: placas de vídeo e processadores de computadores e smartphones; dispositivos de entrada: relacionam-se à captação de dados (escritos, orais ou visuais). Exemplos: teclados, microfones e webcam; dispositivos de saída: fornecem uma interface destinada ao conhecimento ou captação, para outros dispositivos, da informação (escrita, oral ou visual) produzida no processamento. Exemplos: impressoras e monitores; e dispositivos de armazenamento: dizem respeito à guarda de dados ou informações para posterior análise.
>
> Exemplos: pendrives, HDs (hard disks) e CDs (discos compactos).

O aparecimento do crime de Invasão a Dispositivos Informáticos ajudou no desenvolvimento em Leis que fortalecem o poder jurídico,

1.3 Extorsão

O art. 158 do Código Penal, descreve extorsão da seguinte forma:

> Art. 158 - Constranger alguém, mediante violência ou grave ameaça, e com o intuito de obter para si ou para outrem indevida vantagem econômica, a fazer, tolerar que se faça ou deixar de fazer alguma coisa:
> Pena - reclusão, de quatro a dez anos, e multa.
>
> § 1º - Se o crime é cometido por duas ou mais pessoas, ou com emprego de arma, aumenta-se a pena de um terço até metade.
>
> § 2º - Aplica-se à extorsão praticada mediante violência o disposto no § 3º do artigo anterior. Vide Lei nº 8.072, de 25.7.90
>
> § 3o Se o crime é cometido mediante a restrição da liberdade da vítima, e essa condição é necessária para a obtenção da vantagem econômica, a pena é de reclusão, de 6 (seis) a 12 (doze) anos, além da multa; se resulta lesão corporal grave ou morte, aplicam-se as penas previstas no art. 159, §§ 2o e 3o, respectivamente. (Incluído pela Lei nº 11.923, de 2009)

Tem-se penalizado as condutas e praticadas em ambientes virtuais conforme este artigo, pois o crime não é somente o patrimônio e sim também a inviolabilidade da vítima.

Conforme Cléber Masson (2018, p.447):

> A extorsão é crime ofensivo. A lei penal tutela o patrimônio, principalmente, pois o delito está previsto entre os crimes contra o patrimônio, mas não se olvida da integridade física e da liberdade individual, uma vez que para executá-lo o sujeito se vale de grave ameaça ou violência à pessoa.
>
> É preciso destacar que o patrimônio, como bem jurídico protegido pelo art. 158 do Código Penal, há de ser compreendido em sentido mais amplo do que a propriedade e a posse, ao contrário do que se dá no furto e no roubo, pois o tipo penal fala em "indevida vantagem econômica". Destarte, qualquer que seja a vantagem patrimonial obtida ou procurada pelo agente, em detrimento da vítima, estará caracterizado um dos requisitos da extorsão.
>
> De fato, é patrimônio, no contexto do crime em apreço, todo bem ou interesse cujo sacrifício represente, para o seu titular, um mal maior do que o prejuízo patrimonial correspondente à vantagem exigida pelo extorsionário. São exemplos de tais bens ou interesses a honra, a tranquilidade pessoal ou familiar, o crédito comercial etc. Contrariamente ao sustentado pela maioria da doutrina, não consideramos correto classificar a extorsão como crime complexo. Como se sabe, crime complexo é o que resulta da fusão de dois ou mais crimes (exemplos: roubo, latrocínio, extorsão mediante sequestro etc.). E, no terreno do delito tipificado pelo art. 158 do Código Penal, não se verifica tal fenômeno.
>
> Com efeito, a extorsão nada mais é do que uma espécie do gênero "constrangimento ilegal" C, art. 146: é o constrangimento ilegal qualificado pelo fim de indébita locupletarão e que, por isso mesmo, é trasladado para a órbita dos crimes contra o patrimônio. Núcleo do tipo é "constranger", exatamente como no constrangimento legal, e no restante da descrição da conduta criminosa não se verifica a presença de nenhum outro comportamento que, por si só, constitua crime autônomo. Trata-se, portanto, de um constrangimento ilegal com finalidade específica. E nada mais.

Conclui-se que a extorsão, apesar de ser um crime contra o patrimônio, pode perfeitamente ser cometida no ambiente cibernéticos.

1.4 Estelionato

O crime de Estelionato está no art. 171 do Código Penal, disposto da seguinte forma:

> 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. § 2º - Nas mesmas penas incorre quem:
> Disposição de coisa alheia como própria
>
> I - Vende, permuta, dá em pagamento, em locação ou em garantia coisa alheia como própria;
> Alienação ou oneração fraudulenta de coisa própria
>
> II - Vende, permuta, dá em pagamento ou em garantia coisa própria inalienável, gravada de ônus ou litigiosa, ou imóvel que prometeu vender a terceiro, mediante pagamento em prestações, silenciando sobre qualquer dessas circunstâncias;
> Defraudação de penhor
>
> III - Defrauda, mediante alienação não consentida pelo credor ou por outro modo, a garantia pignoratícia, quando tem a posse do objeto empenhado; Fraude na entrega de coisa
> IV - Defrauda substância, qualidade ou quantidade de coisa que deve entregar a alguém;
> Fraude para recebimento de indenização ou valor de seguro
>
> V - Destrói, total ou parcialmente, ou oculta coisa própria, ou lesa o próprio corpo ou a saúde, ou agrava as consequências da lesão ou doença, com o intuito de haver indenização ou valor de seguro; Fraude no pagamento por meio de cheque
> VI - Emite cheque, sem suficiente provisão de fundos em poder do sacado, ou lhe frustra o pagamento.
> § 3º - A pena aumenta-se de um terço, se o crime é cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência.
>
> Estelionato contra idoso
>
> § 4º Aplica-se a pena em dobro se o crime for cometido contra idoso. (Incluído pela Lei nº 13.228, de 2016)

Ainda, conforme Guilherme de Souza Nucci (2017, p. 513):

> O estelionato é um crime artístico, pois implica representação, convencimento, falas decoradas, cenários montados, figurantes e todos os aparatos necessários para enganar alguém com uma história; a única diferença de uma peça teatral bem produzida, que também conta uma história fictícia ou inspirada em fatos reais, é que o estelionatário, ao final, não recebe aplausos, mas ganha uma vantagem ilícita em detrimento da vítima, que se deixou iludir.

O criminoso se utiliza de meio ardil ou qualquer outro meio para roubar ou enganar a vítima. Segundo Rogério Sanches: “Tutela-se com a incriminação do estelionato a inviolabilidade patrimonial, aviltada pela prática de atos enganosos pelo agente”.

Cléber Masson demonstra:

> Artifício é a fraude material. O agente utiliza algum instrumento ou objeto para enganar a vítima. Exemplo: “A” veste-se com o uniforme de uma oficina mecânica para que “B” voluntariamente lhe entregue seu automóvel.
>
> Ardil, por seu turno, é a fraude moral, representada pela conversa enganosa. Exemplo: “A”, alegando ser especialista em relógios automáticos, convence “B” a entregar-lhe seu relógio para limpeza de rotina.

Para a punição do estelionato utiliza o Código Penal para punição da maioria dos crimes cibernéticos que são ocorridos em um ambiente virtual.

1.5 Registro não autorizado da intimidade sexual

O crime de registro não autorizado da intimidade sexual do artigo 216-B do Código Penal, esta dispondo:

> Art. 216-B. Produzir, fotografar, filmar ou registrar, por qualquer meio, conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado sem autorização dos participantes: (Incluído pela Lei nº 13.772, de 2018) Pena - detenção, de 6 (seis) meses a 1 (um) ano, e multa.
>
> Parágrafo único. Na mesma pena incorre quem realiza montagem em fotografia, vídeo, áudio ou qualquer outro registro com o fim de incluir pessoa em cena de nudez ou ato sexual ou libidinoso de caráter íntimo. (Incluído pela Lei nº 13.772, de 2018)

O crime em comento adveio da Lei 13.772 de 2018 (Lei Maria da Penha).

Rogério Sanches Cunha (2018 p. 10-12) descreve este assunto:

> Objetividade jurídica: é a tutela da intimidade, tanto que a mesma lei que insere o art. 216-B institui nos crimes contra a dignidade sexual um capítulo denominado
> “Da exposição da intimidade sexual”.
>
> O tipo preenche a lacuna que existia em relação à punição da conduta de indivíduos que registravam a prática de atos sexuais entre terceiros. Foi a grande repercussão quando, em janeiro de 2018, um casal alugou um apartamento para passar alguns dias no litoral de São Paulo e, depois se instalar, percebeu uma pequena luz atrás de um espelho que guarnecia o quarto. O inusitado sinal faz com que um deles vistoriasse o espelho e, espantado, descobrisse que ali há uma câmera instalada. O equipamento foi imediatamente desligado e, logo em seguida, o casal recebeu uma ligação do proprietário do imóvel, que indagou se havia ocorrido algum problema, o que indicava que as imagens estavam sendo transmitidas em tempo real.
>
> Embora se tratasse de conduta violadora da intimidade e que inequivocamente dava ensejo a indenização por danos morais, o ato – não tão incomum – de quem instalava um equipamento de gravação nas dependências de um imóvel para captar imagens sem o consentimento dos ocupantes não se subsumia a nenhum tipo penal. A partir de agora, é classificado como crime contra a dignidade sexual.
>
> (CUNHA, Rogério Sanches. Breves comentários às Leis 13.769/2018, 13.771/2018, e 13.772/2018.

1.6 Pornografia infantil

É importante destacar que não existe um crime específico que pode ser definido como "pornografia infantil", mas é um termo atribuído no art. 240 até 241-E do Estatuto da Criança e do Adolescente.

No contexto da obra " Prática o Estatuto da Criança e do Adolescente" do professor Claudino de Araújo Júnior descreve algumas jurisprudências relatadas abaixo:

> A consumação do ilícito previsto no art. 241 do Estatuto da Criança e do Adolescente ocorre no ato de publicação das imagens pedófilo-pornográficas, sendo indiferente a localização do provedor de acesso à rede mundial de computadores onde tais imagens encontram-se armazenadas, ou a sua efetiva visualização pelos usuários. (STJ, CC 29.886-SP, Min. Maria Thereza de Assis Moura, 3ª Seção, DJ 12.12.2007).
>
> É da Justiça Federal a competência para o processamento do crime previsto no art. 241-A da Lei nº 8.069/1990, quando a divulgação de imagens e vídeos se dá em perfis públicos sitiados em redes sociais, tornando-as disponíveis para um número indefinido de pessoas e, ao menos potencialmente, para usuários residentes fora do território nacional. (STJ, CC 147.681/RJ, Min. Rogerio Schietti Cruz, DJe 04.10.2016).
>
> É típica a conduta de fotografar cena pornográfica (art. 241-B do ECA) e de armazenar fotografias de conteúdo pornográfico envolvendo criança ou adolescente (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 peças de roupas –, e de poses nitidamente sensuais, em que explorada sua sexualidade com conotação obscena e pornográfica. (STJ, Resp. 1.543.267/SC, Min. Maria Thereza de Assis Moura, DJe 16.02.2016)
>
> Considerando a proibição de analogia ou de interpretação extensiva em prejuízo do réu, a jurisprudência desta Corte firmou-se no sentido de que, somente foi elencado como sujeito ativo do art. 244-A do Estatuto da Criança e do Adolescente o agente que efetivamente sujeita a criança ou adolescente à prostituição, sendo necessária a descrição, na denúncia, de uma conduta que, por meio do emprego de mecanismos de pressão, leve a criança ou adolescente à prostituição. Além disso, os conceitos de prostituição ou de exploração sexual não se coadunam com a ideia de fato isolado, mas sim com a concepção de comportamento que se projeta ou reitera no tempo. Precedentes. (STJ, HC 347.895/GO, Min. Antônio Saldanha Palheiro, DJe 21.09.2016)
>
> Sumula nº 500 do STJ: "A configuração do crime do art. 244-B do ECA independe da prova da efetiva corrupção do menor, por se tratar de delito formal".
>
> É assente no Superior Tribunal de Justiça, bem como no Supremo Tribunal Federal, o entendimento de que o crime tipificado no art. 244-B do Estatuto da Criança e do Adolescente é formal, ou seja, a sua caracterização independe de prova da efetiva e posterior corrupção do menor. (STJ, AREsp 689.567/ PR, Min. Sebastião Reis Júnior, DJe 17.03.2016)

CAPITULO 2 – INTERNET & FERRAMENTAS UTILIZADAS PELOS INFRATORES

A presente seção depreende-se como objetivo a conceituação do que se trata esse ambiente virtual, como também, visa-se a abordagem em torno da internet em seus distintos campos, por meio de aparatos e ferramentas, esses usados de forma invasiva para que o crime ocorra, desde a invasão de privacidade até casos mais graves como de extorsão. Assim, é de suma importância que sejam expostas as várias atuações criminosas, aprofundando-se acerca das técnicas, dos métodos, dos recursos e das ferramentas que os criminosos fazem uso para conseguir seus objetivos ilegais.

2.1 Internet:

A internet surge dentro do contexto da Guerra Fria, com objetivo de comunicação entre as forças militares, estabelecendo comunicação, ou seja, tal ferramenta possui natureza não comercial, já que os EUA, a partir de tal tecnologia, frisava-se estar um passo à frente na disputa e não sofrer com ataques surpresos.

Preceitua Castells (2003, p. 16):

> As origens da Internet podem ser encontradas na Arpanet, uma rede de computadores montada pela Advanced Research Projects Agency (ARPA) em setembro de 1969. A ARPA foi formada em 1958 pelo Departamento de Defesa dos Estados Unidos com a missão de mobilizar recursos de pesquisa, particularmente do mundo universitário, com o objetivo de alcançar superioridade tecnológica militar em relação à União Soviética na esteira do lançamento do primeiro Sputnik em 1957. A Arpanet não passava de um pequeno programa que surgiu de um dos departamentos da ARPA, o Information Processing Techniques Office (IPTO), fundado em 1962 com base numa unidade preexistente. O objetivo desse departamento, tal como definido por seu primeiro diretor, Joseph Licklider, um psicólogo transformado em cientista da computação no Massachusetts Institute of Technology (MIT), era estimular a pesquisa em computação interativa. Como parte desse esforço, a montagem da Arpanet foi justificada como uma maneira de permitir aos vários centros de computadores e grupos de pesquisa que trabalhavam para a agência compartilhar on-line tempo de computação.

Ademais, a popularização da internet ocorreu por intermédio do World Wide Web, ou mais conhecido WWW. Diante desse sistema de hipertexto, houve uma explosão no meio social, de modo que a internet foi se tornando muito utilizada pela sociedade.

Para melhor explanação do assunto, preceitua Castells (2003, p.16):

> O que permitiu à Internet abarcar o mundo todo foi o desenvolvimento da www. Esta é uma aplicação de compartilhamento de informação desenvolvida em 1990 por um programador inglês, Tim Berners-Lee, que trabalhava no CERN, o Laboratório Europeu para a Física de Partículas baseado em Genebra. Embora o próprio Berners Lee não tivesse consciência disso (Berners-Lee, 1999, p.5), seu trabalho continuava uma longa tradição de ideias e projetos técnicos que, meio século antes, buscara a possibilidade de associar fontes de informação através da computação interativa. Vannevar Bush propôs seu sistema Memex em 1945. Douglas Engelbart projetou seu On-Line System, a que não faltavam interface gráfica e mouse, trabalhando a partir de seu Augmentation Research Center na área da Baía de São Francisco, e demonstrou-o pela primeira vez em 1968. Ted Nelson, pensador independente, radical, anteviu um hipertexto de informação interligada em seu manifesto de 1963, Computer Lib, e trabalhou muitos anos na criação de um sistema utópico, Xanadu: um hipertexto aberto, auto evolutivo, destinado a vincular toda a informação passada, presente e futura do planeta. Bill Atkinson, o autor da interface gráfica do Macintosh, desenvolveu um sistema HyperCard de interligação de informação quando trabalhava na Apple Computers na década de 1980.

Portanto, a internet historicamente se relaciona com os contextos revolucionários, de maneira em que tal tecnologia opera no mundo de forma impactante, visto que se tornou tão central na vida das pessoas que é impossível conceber a ideia de uma sociedade com sua ausência, posto que todas as relações atuais se atravessam por meio desse aparato. Sendo assim, faz-se inegável a importância dos esforços para que ocorra a construção de um meio virtual mais seguro para todos os usuários da web, como também às empresas e instituições.

2.2 Técnicas, métodos, recursos e ferramentas utilizadas pelos infratores

Primeiramente, cabe realizar a distinção de hacker e cracker, tal diferenciação se dá pela conceituação dessas. O primeiro grupo se estabelece como estudiosos que realizam análises dos sistemas, com enfoque nas falhas dos sistemas e na vulnerabilidade dessas interfaces. Diante disso, cabe citar que tal prática pode ser feita dentro da lei, contribuindo para o fortalecimento

desses espaços virtuais. Outrossim, tem-se os crackers, esses operam dentro da ilegalidade, pois buscam obter vantagem prejudicial, de maneira em que agem de forma criminosa por meio das brechas para que consigam ganhos ilícitos.

Vale a pena descrever Rogério Greco (2013, p.1):

> Aquele que tem conhecimento e habilidade suficientes para violar mecanismos de segurança, invadindo dispositivo informático alheio, é chamado de hacker. Conforme lições de Sandro D'Amato Nogueira, "este indivíduo em geral domina a informática, é muito inteligente, adora invadir sites, mas na maioria das vezes não com a finalidade cometer crimes; costumam se desafiar entre si, para ver quem consegue invadir tal sistema ou página na internet, isto apenas para mostrar como estamos vulneráveis no mundo virtual".
>
> Por outro lado, existe, também, a figura do cracker, que, ainda de acordo com os ensinamentos de Sandro D'Amato Nogueira, é aquele que "usa a internet para cometer crimes, fraudes bancárias e eletrônicas, furto de dados, golpes e grandes estragos. São verdadeiras
>
> Quadrilhas de jovens que não se contentam apenas em invadir um sistema, usam sua inteligência e domínio da informática para causar prejuízos de milhares de reais, tanto contra pessoas físicas, como jurídicas, órgãos públicos etc.
>
> Diversas são as técnicas, métodos, recursos e/ou ferramentas existentes e que são utilizadas pelos criminosos para o cometimento de delitos virtuais e/ou cometidos em ambientes virtuais, porém serão explanadas as tidas como mais relevantes relacionadas com a finalidade deste trabalho.
>
> No entanto, apesar de que muitas dessas técnicas, métodos recursos e ferramentas existentes possuam propósito malicioso, nada impede que sejam utilizadas para outros fins diversos. Cabe observar também que algumas delas não possuem finalidade maliciosa e sim determinadas pessoas as utilizam para o cometimento de crimes.

2.2.1 Malware

Em primeira análise, vale ressaltar que o recurso Malware é destaque para a temática, visto que se trata de softwares projetados para uma finalidade maliciosa e por ser o principal recurso para realização de atos criminais. Para tal conceituação, foi preciso fazer uso da descrição de Moisés de Oliveira Cassanti (2014 p. 8):

> Termo malware é a contração de "malicious software" programa malicioso e identifica qualquer programa desenvolvido com o propósito de causar dano a um computador, sistema ou redes de computadores. É um dos tipos de intrusos que podem invadir o seu computador (o outro é o próprio atacante). Os mais comuns são os vírus, worms e

> cavalos de troia. Geralmente se utilizam de ferramentas de comunicação conhecidas para se espalharem – como, por exemplo, worms enviados por e-mail e mensagens instantâneas, cavalos de troia provenientes de websites e arquivos infectados por vírus obtidos por downloads de conexões ponto-a-ponto. O malware também tenta explorar as vulnerabilidades existentes nos sistemas, tornando sua entrada discreta e fácil.

A partir disso, os demais recursos elaborados se derivam dos malwares, cada qual sendo reproduzido de uma forma diferente, com objetivo de se aproveitar de determinada brecha.

1.2.2 Vírus e Trojan

O popular termo vírus opera dentro do meio virtual, por meio de lacunas no sistema, são arquivos prejudiciais que transitam pelas redes. Desse modo, os usuários, que geralmente não possuem conhecimento técnico na área de informática, estão sujeitos a acessarem esses arquivos e, assim, colocando-se em risco. Para tanto, faz-se imprescindível o uso de antivírus e outros programas de segurança. Por outro lado, há os trojans, esses malwares operam de maneira camuflada para acessar o aparelho alvo, de modo que são conhecidos como "Cavalo de Tróia". Para esse último, cabe trazer a conceituação feita por Damásio de Jesus (2016 p.35):

> Espécie de malware. Programa que faria algo além do que parece. "Cavalo de troia" é uma instrução ou código malicioso comumente ocultado em outro software, que, instalado, torna um computador ou sistema vulnerável ou mesmo explora vulnerabilidades já existentes. Dependendo do trojan, é possível não só acessar um sistema, como se tornar administrador, copiar informações confidenciais. Muito comum o uso de trojan em phishing scam (e-mails maliciosos que falsificam a identidade visual de instituições e induzem usuários a clicar nestes códigos maliciosos, momento em que são infectados, ou spear phishing, que é o phishing direcionado, focado em um grupo ou organização específicos. Programas como binders, joiners e packers podem compactar um trojan ou inseri-lo juntamente ao outro programa comum e inofensivo, com um game e até mesmo uma apresentação de slides.

Para tais, recomenda-se a atualização dos programas usados com a finalidade de proteção do aparelho e dispositivo do usuário.

CAPITULO 3 - LEGISLAÇÃO BRASILEIRA

O presente capítulo propõe expor as principais Leis no tocante aos crimes cibernéticos.

3.1 Código Penal

Muitos desses crimes estão apresentados no Decreto-Lei Nº 2.284 de 1940 do Código Penal). Reforçando essa ideia, segundo o professor Cléber Masson: “A legislação penal brasileira sempre possuiu arsenal para combater a imensa maioria dos crimes eletrônicos, algo em torno de 95%”.

3.2 Lei nº 11.829 de 2008

O objetivo da Lei está na proteção da criança e do adolescente

Segundo:

> Altera a Lei no 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet.
>
> O PRESIDENTE DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:
>
> Art. 1º Os arts. 240 e 241 da Lei no 8.069, de 13 de julho de 1990, passam a vigorar com a seguinte redação:
>
> “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.
>
> “Art. 241. Vender ou expor venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena – reclusão, de 4 quatro a 8 oito anos, e multa. ”

Art. 2º A Lei no 8.069, de 13 de julho de 1990, passa a vigorar acrescida dos seguintes arts. 241-A, 241-B, 241-C, 241-D e 241-E:

"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:

Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.

§1º Nas mesmas penas incorre quem:

I – Assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;
II – Assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.
§2º As condutas tipificadas nos incisos I e II do § 1o deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo. Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:

Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.

§1º A pena é diminuída de 1 (um) a 2/3 (dois terços) se de pequena quantidade o material a que se refere o caput deste artigo.

§2º Não há crime se a posse ou o armazenamento tem a finalidade de comunicar às autoridades competentes a ocorrência das condutas descritas nos arts. 240, 241, 241A e 241-C desta Lei, quando a comunicação for feita por:

I – Agente público no exercício de suas funções;
II – Membro de entidade, legalmente constituída, que inclua, entre suas finalidades institucionais, o recebimento, o processamento e o encaminhamento de notícia dos crimes referidos neste parágrafo;
III – Representante legal e funcionários responsáveis de provedor de acesso ou serviço prestado por meio de rede de computadores, até o recebimento do material relativo à notícia feita à autoridade policial, ao Ministério Público ou ao Poder Judiciário.
§ 3º As pessoas referidas no § 2o deste artigo deverão manter sob sigilo o material ilícito referido.

Art. 241-C. Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual: Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Incorre nas mesmas penas quem vende, expõe à venda, disponibiliza, distribui, publica ou divulga por qualquer meio, adquire, possui ou armazena o material produzido na forma do caput deste artigo.

Art. 241-D. Aliciar, assediar, instigar ou constranger, por qualquer meio de comunicação, criança, com o fim de com ela praticar ato libidinoso:

Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.

Parágrafo único. Nas mesmas penas incorre quem:

> I – Facilita ou induz o acesso à criança de material contendo cena de sexo explícito ou pornográfica com o fim de com ela praticar ato libidinoso;
> II – Pratica as condutas descritas no caput deste artigo com o fim de induzir criança a se exibir de forma pornográfica ou sexualmente explícita.
> Art. 241-E. Para efeito dos crimes previstos nesta Lei, a expressão "cena de sexo explícito ou pornográfica" compreende qualquer situação que envolva criança ou adolescente em atividades sexuais explícitas, reais ou simuladas, ou exibição dos órgãos genitais de uma criança ou adolescente para fins primordialmente sexuais. " Art. 3º Esta Lei entra em vigor na data de sua publicação.
>
> Brasília, 25 de novembro de 2008; 187º da Independência e 120º da República.

A Lei ajuda a combater estas práticas ilegais e criminosas.

3.3 Lei nº 12.735 de 2012

Esta Lei foi alterada no Decreto-Lei nº 2.848 de 1940 (Código Penal), no Decreto Lei no 1.001 de 1969 (Código Penal Militar) e na Lei nº 7.716 de 1989.

Descreve a Lei:

> Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.
>
> A PRESIDENTA DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:
>
> Art. 1º Esta Lei altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.
>
> Art. 2º (VETADO)
>
> Art. 3 º (VETADO)
>
> Art. 4º Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.
>
> Art. 5º O inciso II do § 3o do art. 20 da Lei nº 7.716, de 5 de janeiro de 1989, passa a vigorar com a seguinte redação:
> "Art.20.....
> .....§3º.....

> .....”
>
> II - a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio;
>
> .....”
>
> Art. 6º Esta Lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação oficial.
>
> Brasília, 30 de novembro de 2012; 191º da Independência e 124º da República.

3.4 Lei 12.737 de 2012

Conforme a Lei: “Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e de outras providências” (lei nº 12.737, de 30 de novembro de 2012).

Contudo, importante salientar, para enriquecimento introdutório, que, preceitua Damásio de Jesus (2016 p.85):

> Apelidada de “Lei Carolina Dieckmann”, a Lei n. 12.737/2012, que tipifica os crimes cibernéticos, adveio do Projeto de Lei n. 2.793/20115, sendo agilizado no início de 2013 pelo “casuísmo em que fotos íntimas da atriz teriam sido supostamente copiadas de seu computador e divulgadas na internet”. Na verdade, a legislação veio atender a uma demanda antiga do setor financeiro, duramente impactado com os golpes e fraudes eletrônicas, ainda que considerada uma lei absolutamente “circunscrita”, em comparação aos projetos sobre crimes cibernéticos que tramitavam no congresso nacional. Entendeu-se em aprovar uma lei menor, com pontos menos polêmicos, a não ter nada regulamentando crimes cibernéticos, eis que, diz o ditado, a lei é como remédio, deve ser ministrado em doses, pois se ministrarmos tudo de uma vez, podemos matar o paciente.

Os seguintes crimes ao Código Penal foram acrescentados: Invasão de dispositivo informático (Art. 154-A); Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública (Art. 266); Falsificação de documento particular, Falsificação de cartão (Art. 298), citado 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: (Incluído pela Lei nº 12.737, de 2012) Vigência
>
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. (Incluído pela Lei nº 12.737, de 2012) Vigência
>
> §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. (Incluído pela Lei nº 12.737, de 2012) Vigência
>
> §2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico. (Incluído pela Lei nº 12.737, de 2012) Vigência
>
> §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: (Incluído pela Lei nº 12.737, de 2012) Vigência
>
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave. (Incluído pela Lei nº 12.737, de 2012) Vigência
>
> §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 obtidas. (Incluído pela Lei nº 12.737, de 2012) Vigência
>
> §5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
>
> (Incluído pela Lei nº 12.737, de 2012) Vigência
>
> Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:
>
> Pena - reclusão, de um a cinco anos, e multa.
>
> Falsificação de cartão (Incluído pela Lei nº 12.737, de 2012) Vigência
>
> Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito. (Incluído pela Lei nº 12.737, de 2012) Vigência

2.5 Lei nº 12.965 de 2014

Conforme Victor Hugo Pereira Gonçalves: “ Marco Civil é uma legislação cujo objetivo precípuo é o de regular as relações sociais entre os usuários de internet. ”

Conhecida como Marco Civil da Internet a Lei 12.965/14 recebeu o apelido de “Constituição da Internet”.

Estados, do Distrito Federal e dos municípios em relação matéria. ” Lei nº 12.965 de 2014. Complementado, segundo Damásio de Jesus (2016 p. 168):

> Marco civil da internet é considerado a “constituição da internet”, garantindo direitos e deveres a todos os atores da internet Brasileira usuários, provedores de conexão e de servi os em geral. Fruto de um projeto nascido em 29 de outubro de 2009, da secretaria de Assuntos Legislativos do Ministério da Justiça, em parceria com a Escola de Direito do Rio de Janeiro da Fundação Getúlio Vargas, o Marco civil foi uma construção colaborativa, disponível para consulta pública entre novembro de 2009 e junho de 2010, tendo recebido mais de duas mil contribuições1. Após a fase de participação popular, ingressou no congresso em 24 de agosto de 2011, por meio do Projeto de Lei n. 2.126, de iniciativa do Poder Executivo, projeto que visou estabelecer princípios, garantias, direitos e de- veres para o usuário da internet no Brasil. A legislação tem escopo de evitar, igualmente, decisões contraditórias proferidas pelo Judiciário, em casos semelhantes envolvendo tecnologia da informação, gerando insegurança jurídica. Foi sancionado pela Presidência da República em 23 de a abril de 2014, tornando-se a Lei n. 12.965. Cogita-se, ainda, da propositura na Assembleia das nações Unidas de um possível Marco civil internacional. O Marco civil da internet pode ser integrado s leis e Projeto de estudo neste livro. São complementares nas atividades envolvendo repressão a crimes cibernéticos (JESUS, Damásio de, 2016, p. 168).

2.6 Lei nº 13.772 de 2018

A Lei nº 13.722/2018, novidade do ano de 2018 e vem ao encontro aos crimes cibernéticos alterando o Código Penal e a Lei nº 11.340/2006 (Lei Maria da Penha). Destaca:

> LEI Nº 13.772, DE 19 DE DEZEMBRO DE 2018.
>
> Altera a Lei no 11.340, de 7 de agosto de 2006 (Lei Maria da Penha), e o Decreto Lei no 2.848, de 7 de dezembro de 1940 (Código Penal), para reconhecer que a violação da intimidade da mulher configura violência doméstica e familiar e para criminalizar o registro não autorizado de conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado.
>
> O PRESIDENTE DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:
>
> Art. 1º Esta Lei reconhece que a violação da intimidade da mulher configura violência doméstica e familiar e criminaliza o registro não autorizado de conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado.

Art. 3º O Título VI da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), passa a vigorar acrescido do seguinte Capítulo I-A:

CAPÍTULO I-A

DA EXPOSIÇÃO DA INTIMIDADE SEXUAL

Registro não autorizado da intimidade sexual

Art. 216-B. Produzir, fotografar, filmar ou registrar, por qualquer meio, conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado sem autorização dos participantes:

Pena - detenção, de 6 (seis) meses a 1 (um) ano, e multa.

Parágrafo único. Na mesma pena incorre quem realiza montagem em fotografia, vídeo, áudio ou qualquer outro registro com o fim de incluir pessoa em cena de nudez ou ato sexual ou libidinoso de caráter íntimo. ”

Art. 4º Esta Lei entra em vigor na data de sua publicação.

Brasília, 19 de dezembro de 2018; 197º da Independência e 130º da República.

MICHEL TEMER

Torquato Jardim

Gustavo do Vale Rocha

Raul Jungmann

Este texto não substitui o publicado no DOU de 20.12.2018

Trata-se de uma Lei recente

CAPITULO 4 - JURISPRUDÊNCIA A RESPEITO DOS CRIMES VIRTUAIS

No Brasil a legislação descreve os crimes cibernéticos precisa evoluir conforme visto no capítulo anterior. Serão expostas algumas jurisprudências pertinentes aos crimes cibernéticos.

4.1 Jurisprudências

Crime de furto qualificado cometido na rede mundial de computadores:

As alegações da " Lovatio Legis" localiza-se exatamente como ocorreu o crime de estelionato cibernético e virtual, na alta das fraudes virtuais por meio do aumento da utilização das atividades pessoais e profissionais dos meios de comunicação e dispositivos para trabalho e lazer e nas realizações de crimes, teve uma correlação expressiva no uso de meios maliciosos dos dispositivos eletrônicos e programas para roubar dados bancários , pra benefício próprio e lucro absurdo subtraindo, invadindo essas contas bancarias, mediante essas ações qualifica as de crime de furto qualificado pois os agentes usam de a internet como ferramenta para concluir o delito , em tese os tipos penais previstos dos artigos 155 , parágrafo 4° , inciso II e IV e também 288 , ambos do Código Penal , no artigo 10 da lei n ° 9.296/1996 , no artigo da lei complementar n° 9.613/98 ,uma novidade digna é nova redação do art. 154-A do Código Penal, se refere à propriedade do dispositivo informático. A redação anterior falava em "dispositivo informático alheio", indicando que o sujeito ativo deveria violar um dispositivo pertencente a outra pessoa. A nova redação empregou a expressão "dispositivo informático de uso alheio", indicando que o crime se configura ainda que o sujeito ativo viole o seu próprio dispositivo informático, de sua propriedade, que esteja sendo utilizado. Pela vítima a qualquer título (empréstimo, por exemplo). Logo, o sujeito ativo pode ser o próprio dono do dispositivo.

Voltando à análise do furto, há que se distinguir o crime de furto mediante fraude por meio de dispositivo eletrônico ou informático do crime de estelionato cibernético ou virtual.

Trata-se de crime virtual em que os criminosos foram enquadrados na conduta de furto qualificado.

A jurisprudência abaixo descreve o crime contra a honra:

Os crimes contra honra, nos grupos do aplicativo de comunicação, WhatsApp ; gera sim indenizações , punições , por se tratar de um meio de comunicação rápida , a velocidade que se propaga é absurda ,podendo atribuir falsamente com uma calunia , difamação , atribuindo fatos desnecessários ferindo a honra e amoral de indivíduos, injuria, um aborrecimento que fere , e apesar de fugir dos padrões, toda via sendo em ambiente virtual deve se espelhar no disposto artigo 70 , do Código de Processo Penal , que tem a competência de julgar a imputação de injúria , mediante a publicação ofensiva nas redes sociais , nesse caso acima o delito foi pela plataforma WhatsApp ,em grupo privado. Demonstra crimes causados por um aplicativo de celular muito conhecido e utilizado pelo público que é o WhatsApp.

A jurisprudência descreve um crime virtual bancário:

Mesmo com o advento do pacote ante crimes , é uma aventura se desviar desses golpes , pois a velocidade e a inteligência artificial desses programas que são usados nos roubos de dados , são incompatíveis com o conhecimento do cidadão comum e são os que caem com mais facilidade nesses golpes , pois sem malicia , acaba baixando pacotes que veem com propagandas e ali existe um vírus no qual muitas vezes os próprios usuários facilita a instalação , e nesse momento os vírus já instalado , fazem o trabalho sujo , com a certeza da impunidade vai gerando danos financeiros a milhares de pessoas , um roubo que está se tornando comum , pois os usuários sem habilidades acabam fornecendo a abertura para que o delito ocorra ,sem se prevenir .

Muitos chegam aos tribunais e até perdem as ações contra os bancos, pois tem atitudes que infelizmente depende dos usuários, e os aparelhos usados é da própria vítima. Alguns deixam de lado, e como esse tipo de crime depende da representação da vítima, sem a reclamação oficial torna se uma problemática nas investigações. Configurado no artigo 171 do Código Penal e a Lei 14.155 que altera o Código Penal para punição de crimes digitais.

A vítima em questão caiu em uma fraude em ambiente virtual. Portanto podemos reforçar novamente que o público deve estar atento às medidas básicas de segurança para navegar na internet para evitar maiores transtornos econômicos e pessoais.

CONSIDERAÇÕES FINAIS

Na primeira fase do trabalho, foi mostrado tecnicamente o modo como é conhecido e utilizado os crimes cibernéticos de forma simples para que haja fácil compreensão, assim, evidencia-se os recursos e as ferramentas para o ato ilícito. Em seguida, há a explanação técnicas dos métodos criminosos na aplicação dos crimes cibernéticos. Foi exposto ainda a nossa Legislação, denota-se a criação de leis, a fim de impedir o progresso desses crimes, assim como a sua perpetuação.

Aborda-se a aplicação das Leis através de um conjunto de jurisprudenciais dos crimes cometido em nosso país, para tal confirmação, é válido acessar o site do congresso.

Em uma consideração final, pondero de maneira positiva o progresso das criações das Leis contra as impunidades provocadas por estes crimes sob a luz do código penal, com intuito de punir os criminosos virtuais.

É claro que a nossa legislação necessita de leis específicas para que não haja espaço oportuno para novas ações virtuais na criação de uma conduta criminosa e suas tipificações.

Os referidos crimes podem ser praticados por qualquer pessoa, porém existem indivíduos específicos tais como os crakers.

Todavia ainda existem lacunas na nossa legislação que tipificam todas as condutas criminosas no âmbito virtual, o que, de fato, dificulta a punição dos infratores e aplicação do código penal.

No Brasil, recentemente foi aprovado a Lei n. º 12.695/2014, popularmente conhecida como Marco Civil da Internet, que trouxe inúmeros avanços quanto aos direitos e deveres dos usuários e provedores da internet.

Apesar de tudo, o nosso país tem avançado dentro desse cenário, à medida que a expectativa futura reverbera de forma positiva na criação de novas leis específicas para que o combate ao crime cibernético, assim como o aumento de investimentos de proteção na segurança das informações dos dados dos usuários se torne presente cada dia mais dentro do Código Penal.

E a inexistência da culpabilidade pelos crimes de internet preocupa pois consiste em regulamentar e fundamentar juridicamente esses delitos, criando uma parcialidade individual para culpa do agente causador do dano.

Sabemos que na ausência de uma legislação específica, o indivíduo que praticou o ato ilícito no ambiente virtual deverá ser assim, julgado dentro do próprio Código Penal mantendo uma assimetria. A internet se tornou uma asseveração de um futuro melhor para humanidade, por ser algo ímpar e de instrumento de remodelamento de aprendizado constante e a liberdade que a internet da aos usuários sendo um imenso mundo sem fronteiras e por isso o Direito Penal consiste em prescindir as condutas divergentes da nossa normativa. Essa normatividade tem uma dupla função que é coibir o crime e aos mesmo tempo gerando uma expectativa de que as leis sejam cumpridas diminuindo os delitos.

REFERÊNCIAS

BIANCHINI, Alice; GOMES, Luiz Flávio. **Crimes informáticos e suas vítimas;** 2ª ed**.** Editora Saraiva, 2015.

BRASIL. **Decreto-lei no 2.848, de 7 de dezembro de 1940; Código Penal.** Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm. Acesso em 21 nov. 2018.

BRASIL**. LEI nº 12.965, de 23 de abril de 2014, Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato20112014/2014/lei/l12965.htm. Acesso em 24 Nov. 2018.

BRASIL. **Lei nº 12.735, de 30 de novembro de 2012, Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências**. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm.
Acesso em: 25 Nov. 2018.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012, Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.** Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm.
Acesso em 25 Nov. 2018.

BRASIL. **Lei nº 2.848, 7 de dezembro de 1940, Decreto Lei 2840/40. Código Penal 154-A.** Disponível em: https://www.jusbrasil.com.br/topicos/28004011/artigo-154a-do-decreto-lei-n-2848-de-07-de-dezembro-de-1940.

Acesso em: 13 Jan. 2019.

BRITO, Auriney. **Direito penal informático**; 1ª ed. Saraiva, 2013

CASSANTI, Moisés de Oliveira; **Crimes Virtuais, Vítimas Reais**; Rio de Janeiro, Ed. Editora Brasport. 2014.

CASTELLS, **Manuel. A galáxia da Internet, reflexões sobre a Internet, os negócios e a sociedade**; 1ª ed. Editora Zahar, 2003;

CARDOZO, José Eduardo; Congresso Nacional. **Lei Carolina Dieckmann**. Lei nº 12.737, de 30 Nov. 2012.

Disponível em: http://www.coaliza.org.br/lei-carolina-dieckmann/. Acesso em: 10 Fev. 2019.

CARDOZO, José Eduardo; Congresso Nacional. **Lei nº 12.735**, de 30 Nov. 2012. Disponível em:

https://www2.camara.leg.br/legin/fed/lei/2012/lei-12735-30-novembro-2012-774689-publicacaooriginal138237-pl.html. Acesso em: 11 Fev. 2019.

CARTILHA, Segurança para internet. **Ataques na Internet**. Mar. 2017. Disponível em: https://cartilha.cert.br/ataques/. Acesso em: 27 Fev. 2019.

CUNHA, Sanches Rogério. **Manual de direito penal parte especial**. 9ª Ed. Editora jusPODVM. 2017.

DAMÁSIO, Jesus de; MILAGRE, José Antônio. **Manual de crimes informáticos.** Editora Saraiva, 2016.

GONÇALVES, Victor Hugo Pereira. **Marco Civil da Internet Comentado**. 1ª Ed. Editora Atlas. 2017.

GRECO, Rogério. **Código Penal Comentado**. 11ª Ed. Editora Impetus. 2017.

GRECO, Rogério. **Invasão de dispositivo informático art. 154 -a do código penal**. 13 Jan 2013. Seção Artigos. Disponível em: https://rogeriogreco.jusbrasil.com.br/artigos/121819872/invasao-de-dispositivoinformatico-art-154-a-do-codigo-penal. Acesso em: 21 Jan. 2019.

MASSON, Cleber. **Direito pena, parte especial**. 11ª ed. Editora Método. 2018.

NUCCI, Guilherme de Souza. **Curso de direito penal parte geral**. 3ª Ed. Editora Forense 2018.

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

REALE, Miguel. **Lições preliminares de direito**. 27ª ed. Editora Saraiva. 2002.

SYDOW, Spencer Toth. Col. Saberes monográficos. **Crimes informáticos e suas vítimas**, 2ª ed. Editora Saraiva. 2015.

WENDT, Emerson; JORGE, Higor Vinícius Nogueira; **Crimes Cibernéticos: Ameaças e procedimentos de investigação**. 2ª Ed. Editora Brasphort. 2013.