PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE DIREITO E RELAÇÕES INTERNACIONAIS
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO
ARTIGO CIENTÍFICO

CIBERCRIMES

A VULNERABILIDADE DOS USUÁRIOS

ORIENTANDO (A) – MILENA ANGELA SANTOS LIMA
ORIENTADOR (A) - PROF. ME. JOSÉ HUMBERTO ABRÃO MEIRELES

GOIÂNIA-GO
2022

MILENA ANGELA SANTOS LIMA

CIBERCRIMES

A VULNERABILIDADE DOS USUÁRIOS

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUC GOIÁS).

Prof. Orientador: ME José Humberto Abrão Meireles.

GOIÂNIA-GO

2022

MILENA ANGELA SANTOS LIMA

CIBERCRIMES

A VULNERABILIDADE DOS USUÁRIOS

Goiânia, 25 de maio de 2022

BANCA EXAMINADORA

Orientador: Prof. ME José Humberto Abrão Meireles Nota

Examinador (a) Convidado (a): Prof. (a): ME. Eufrosina Saraiva Silva Nota

CIBERCRIMES

A VULNERABILIDADE DOS USUÁRIOS

MILENA ANGELA SANTOS LIMA[1]

O presente artigo buscou analisar os crimes cibernéticos praticados no Brasil correlacionando ao tratamento legal bem como aos meios de combates. Para tanto, o trabalho objetivou tratar das diferentes concepções de cibercrimes, as espécies de crimes cibernéticos mais vulneráveis, a aplicação de normas a estes crimes, além disso, identificou os meios de combates eficazes, a competência para julgar determinados crimes e decisões dos tribunais já existentes no ordenamento jurídico acerca do tema. O estudo teve como base a leitura de artigos e obras cientificas, com menção especial a certos autores como Fernando Capez, Marco Antônio Zanellato, Wanderson Castilho, Jose Antônio Milagre de Oliveira, Pedro Rama, etc. A proposta foi dividir o presente estudo em três capítulos. O primeiro capítulo trata sobre o histórico de cibercrimes, bem como conceitua e classifica as espécies de crimes cibernéticos. Já o segundo capítulo apresenta os tratamentos legais sobre o tema e, por fim, o terceiro capítulo discorre sobre os meios de combate dos crimes cibernéticos.

Palavras-chaves: Crimes. Cibernéticos. Internet. Espécies. Legislação.

[1] Qualificação do autor.

SUMÁRIO

INTRODUÇÃO

Este artigo foi desenvolvido com o intuito de proporcionar elementos para a compreensão dos cibercrimes, abordando seus reflexos no tratamento legal e nos meios de combates. Consequentemente, a aplicação do Direito Penal para coibir a prática de cibercrimes é essencial para a segurança dos usuários, bem como para garantir que ocorra uma aplicação de punições adequadas com escopo de promover a justiça social.

Desse modo, este artigo foi desenvolvido em três capítulos e a metodologia utilizada foi a leitura de artigos e obras cientificas, tendo como base referências bibliográficas de diversos autores, tais como Fernando Capez, Marco Antônio Zanellato, Wanderson Castilho, Jose Antônio Milagre de Oliveira, Pedro Rama e outros.

O primeiro capítulo aborda um breve histórico do surgimento da internet e dos crimes cibernéticos. Ademais, é apresentado o conceito e espécies de cibercrimes, tais como, invasão de privacidade, fraudes virtuais, crimes contra a honra, estelionato e pornografia infantil.

O segundo capítulo apresenta as respectivas legislações nacionais que configura as condutas praticadas pelos cibercriminosos no ambiente virtual. Além disso, trataremos sobre a relevância do Marco Civil da Internet que prevê os princípios, direitos e deveres que regulam o uso adequado da internet no Brasil.

O terceiro capitulo busca esclarecer acerca dos meios jurídicos de combate aos crimes cibernéticos, que envolvem uma dificuldade na produção de provas desses delitos, mormente, observa-se os aspectos relativos à competência para processar e julgar os crimes cibernéticos.

Por fim, o tema, apesar de atual, só recebeu uma atenção adequada em nosso ordenamento jurídico há pouco tempo atrás, haja vista, que a internet tem um espaço considerável em nossas vidas, além de trazer facilidade de comunicação e informações para a sociedade em tempo real. Com isso, como Direito é um conjunto de normas jurídicas estabelecidas para organizar a sociedade, cabe a ele acompanhar o avanço tecnológico e providenciar soluções eficazes para coibir as práticas de crimes cibernéticos.

CAPÍTULO I – CIBERCRIMES

A percepção no que concerne o desenvolvimento da tecnologia, do histórico de informações e das ameaças virtuais que ocorrem diariamente, trazem a sociedade um auxilio no entendimento quanto aos conceitos e espécies de crimes cibernéticos. Deste modo, a relação entre o direito e a internet, além de ser contemporânea, é um meio que traz conflitos virtuais que acontece de forma cada vez mais constante e corriqueira, o que incumbe ao direito a reponsabilidade de ter uma regulamentação eficaz.

1.1 – Histórico/Conceito

Com o fenômeno da globalização, surgiu os computadores, e com isso o termo “Cibernético” tem-se tornado cada vez mais popular. Segundo o dicionário Aurélio, a cibernética consiste na “ciência que estuda os mecanismos de comunicação e de controle nas maquinas e nos seres vivos”, ou seja, tudo que for “Cibernético” está direcionado com o mundo virtual.

A partir daí, a internet é um campo importante de pesquisas, de interatividade para o relacionamento humano, que nos proporciona vários canais de comunicação, que são advindos conforme as tecnologias vão sendo avançadas, e com isso os usuários podem utilizar tais recursos tanto para o bem quanto para o mal. Deste modo, a realidade nos traz uma necessidade de se legislar a cerca do tema, visando alcançar o crescente números de usuários que usam de forma criminosa, prejudicando outros, e assim, trazendo consequências jurídicas.

De acordo com Simas,

> A evolução operada nas novas tecnologias, projetou-se sobre o fenómeno criminal, pois se atendermos às suas duas vertentes, por um lado, a tecnologia poder, ela mesma, objeto de prática de crimes e por outro lado, suscita e potência novas formas criminais ou novas formas de práticas antigos crimes (SIMAS, 2014, p. 14).

Com isso, a internet é uma rede que pode ser utilizada por variados meios de comunicação, *verbi gratia*, smartphones, vídeo games, computadores e, etc. E sua invenção está associada com a criação dos computadores que se deu no ano de 1847, pelo matemático inglês Charles Babbage, que idealizou o primeiro computador do mundo, com objetivo de solucionar as operações aritméticas. (OLIVEIRA JÚNIOR, 2001)

Desde a sua criação, a internet se tornou um canal importante na vida dos usuários, pois, apesar de ser criada com objetivos militares, vem cada vez mais sendo um atrativo para criminosos praticarem crimes, e da mesma forma que a rede fornece facilidades de uso, informações em tempo real, proteção de dados, possibilita também que esses dados sejam vazados, expostos ou adulterados. Sem sombra de dúvidas, as redes não podem ser destruídas por bombardeios, mas podem ser utilizadas pelos criminosos em forma de colocar os usuários vulneráveis.

A partir da década de 1980, a internet se tornou o que é hoje, uma rede que é interligada a milhares de computadores espalhados pelo mundo inteiro, podendo ser utilizadas por todos, e como consequência dessa facilidade, a internet se tornou um espaço para prática de crimes, onde o agente delituoso não necessita mais sair da sua residência para praticar atos ilícitos.

Como afirma Bernado Felipe Estellita Lins

> "Na década de oitenta, a Internet torna-se realidade. Cientistas de diversos países passam a se comunicar diretamente, pelos computadores das universidades e seus terminais. A rede já se expande além das fronteiras dos EUA. Uma curiosidade dos primeiros anos da Internet era a confecção de mapas da rede, com suas centenas de pontos de acesso, permitindo que os usuários pudessem acompanhar seu crescimento e identificar os endereços IP dos seus principais colaboradores." (2013, pg.20)

Entretanto, os crimes cibernéticos tiveram seus primeiros registros a partir do ano de 1960 em diante, com diversos casos de manipulação e sabotagem de sistemas de computadores. Em 1970, a figura do hacker já era referida em razão dos crimes de invasão de sistemas e furto de *softwares*. Em 1980, tais crimes se desenvolveram com a prática de pedofilia, invasão de sistemas, pirataria, vírus, causando então, preocupações maiores com a segurança virtual. (CARNEIRO, 2012)

Na década de 1990, resta afirmado que a internet se tornou uma ferramenta indispensável no dia a dia dos usuários, surgindo assim uma área que merece uma regulação especifica como tantos outros meios de comunicação.

Com o desenvolvimento dos computadores, aumenta-se os números de acessos à internet, tornando-se cada vez mais um meio em que os criminosos atingem os usuários com o auxílio das ferramentas que a própria inovação da tecnologia nos proporciona.

Dito isso, podemos denominar crimes cibernéticos ou cibercrimes todo ato que envolva computadores ou os meios de tecnologia, utilizados pelos criminosos como

objeto de um crime por realizar condutas violadoras de direito privados, que acabam colocando o usuário como vítima de um crime informático.

Como diz Damasio de Jesus e Jose Antonio Milagre (2016, p.09).

> Cibercrime refere-se a “fato típico e antijurídico praticado versus a tecnologia da informação, ou seja, cometido através da informática em geral”

Assim, não há um conceito definido de crimes cibernéticos, nem tão pouco alguma classificação, mas, as condutas são punidas a partir do Código Penal Brasileiro. Nessa mesma perspectiva, alguns autores classificam os crimes cibernéticos como próprios e impróprios, sendo os próprios aqueles que não tem as condutas tipificadas nos tipos penais e os impróprios, por outro lado, são tipificados no ordenamento jurídico.

Por fim, a realização de crimes via internet assume outras expressões, que são: cybercrime, crimes informáticos, crimes digitais, delito informático, crimes virtuais, crimes eletrônicos, além de outros. Contudo, nesse artigo consideraremos em utilizar o termo *Cibercrime*.

1.2 – Espécies de Cibercrimes Impróprios

Nesse tópico, é importante ressaltar que a maioria dos crimes cibernéticos também acontecem no mundo real, e com isso o avanço tecnológico, as condutas delituosas acontecem livremente, sem obstáculos e se espalham rapidamente, dificultando ainda mais para encontrar o agente que praticou.

Sendo assim, existem diversas espécies de crimes cibernéticos, e Augusto Eduardo de Souza Rossini nos ensina que:

> Diferentes tipos de infrações são cometidas pela internet, como: falsificação de dados, estelionatos eletrônicos, pornografia infantil, racismo e xenofobia (difusão de imagens, a discriminação ou a violência contra uma pessoa ou contra um grupo de pessoas, em razão da raça, religião, cor, ascendência, origem nacional ou étnica, injúria e ameaças 8ualificadas pela motivação racista; negação, minimização grosseira, aprovação ou justificação do genocídio ou outros crimes contra a humanidade).

Portanto, nas espécies abordaremos os crimes cibernéticos impróprios, com ênfase nos mais comuns, que são: invasão de privacidade, fraudes virtuais, crimes contra a honra, estelionato e pornografia infantil.

1.2.1 – Invasão de privacidade

O crime de invasão de privacidade consiste em invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita.

A invasão de privacidade nos últimos anos tem sido constante em razão do crescente números de acessos na internet pelo mundo inteiro, consequentemente gerando assim uma movimentação de informações de dados pessoais, em redes sociais, sites que necessitam de cadastros para a realização de compras e, que podem ser um meio fraudulento e utilizados como forma indevida por criminosos.

Deste modo, o Brasil possui uma tipificação penal a essa situação, que com o surgimento da Lei n.12.737/2012, defendeu a punição do delito pela prática de invasão com base no artigo 154-A do Código Penal, e tem como objetivo proteger os dados que os usuários disponibilizam na internet e, por conseguinte o dever do Estado de resguardar os direitos e a identidade dos usuários.

Importante ressaltar que, nesse crime, o elemento subjetivo é o dolo e, não existe a figura culposa do agente, visto que, a mera invasão não é caracterizada como crime, sendo necessário que haja uma finalidade especifica, ou seja, quando o agente consiste obter dados ou informações sem autorização do titular.

1.2.2 – Fraudes virtuais

O crime de fraude virtual previsto no art. 171 do Código Penal nos §§ 2º-A e 2º-B, ocorre quando a invasão, alteração, modificação ou adulteração de dados eletrônicos, por exemplo, o caso da atriz Carolina Dieckmann, que teve seu computador invadido por criminosos, que divulgaram suas fotos intimas nas redes sociais.

Posto isso, nas fraudes virtuais os usuários são incentivados de forma ingênua a fornecerem informações dos seus dados pessoais em páginas, e-mails e mensagens com links fraudulentos nas redes sociais. É por esse meio assombroso que o criminoso comete a ação, agindo intencionalmente com o propósito de obter algum benefício material ou até mesmo financeiro.

Dentre as fraudes virtuais mais comuns, estão o *phishing*, que é um meio antigo, mas bastante utilizado, porque ainda funciona, haja vista, se realiza quando o criminoso passa por uma terceira pessoa para obterem informações pessoais, como por exemplo CPF, senhas, através de sites que fornecem promoções falsas, anúncios para chamar a atenção dos usuários via *WhatsApp*, mas que na realidade, são meios de conseguirem informações da vítima.

Vale ressaltar que um canal que acontece bastante fraudes, é o *WhatsApp*, uma vez que o aplicativo é uma ferramenta que além de ser um canal de mensagens moveis mais usado, possui mais de 2 bilhões de usuários ativos pelo mundo.

1.2.3 – Crimes contra a honra

O crime contra a honra é um direito fundamental protegido pela Constituição Federal em seu artigo 5º, inciso X. De forma especifica, o crime contra a honra consiste na formação de atributos morais, físicos e intelectivos de um indivíduo, que determinam se é merecedora do convívio social ou não dentro da sociedade.

Por se tratar de um crime virtual impróprio, suas tipificações penais já estão previsto no ordenamento jurídico, juntamente com os artigos 138, 139 e 140 do Código Penal, que pune as condutas de caluniar, difamar ou injuriar alguém, que são crimes comuns, mas que praticados por criminosos através do uso da internet.

Segundo a Declaração dos Direitos do Homem e do Cidadão,

> Art. 11º. A livre comunicação das idéias e das opiniões é um dos mais preciosos direitos do homem. Todo cidadão pode, portanto, falar, escrever, imprimir livremente, respondendo, todavia, pelos abusos desta liberdade nos termos previstos na lei.

Desta forma, todos nós somos livres para pensarmos, escolhermos, desde que não atinja ou denigra moralmente a honra do outro. Contudo, a realidade prática se distingue da teoria, pois a realização desses crimes no meio social cresce diariamente e, são em razão de invejas, preconceitos a gêneros de cor e religião, dentre outros, assim, os criminosos utilizam dessa vulnerabilidade para a prática do crime.

Por fim, vale ressaltar que esses crimes, na maioria das vezes, são realizados de forma anônima, mas ainda assim, não deixa de ser uma conduta tipificada, porém se torna ainda mais difícil o policiamento para o reconhecimento do delito.

1.2.4 – Estelionato

O estelionato é um crime que se tornou bastante popular, devido a vários acontecimentos conseguintes do avanço tecnológico. O Código Penal no seu artigo 171, estabelece como estelionato, obter para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artificio, ardil, ou qualquer outro meio fraudulento.

Segundo Rogério Greco,

> "Qualquer meio fraudulento utilizado pelo agente, seja mediante dissimulações, seja até mesmo uma reticência maliciosa, que faça a vítima incorrer em erro, já será suficiente para o raciocínio relativo ao delito de estelionato" (GRECO, 2012, p. 98)

Deste modo, o objetivo do agente que pratica estelionato no meio virtual, será de induzir ou manter a vítima em erro para obter uma vantagem ilícita e causar um prejuízo alheio. Sendo assim, estelionato virtual, são e-mails com links, códigos falsos, no qual o usuário sente se atraído e clica no link que o direciona a um site inexistente, com o intuito de pegar seus dados bancários e transferir valores que está na conta da vítima para si ou para outrem.

1.2.5 – Pornografia infantil

A pornografia infantil está entre as denúncias mais recebidas se comparada aos outros crimes cibernéticos. Nesse sentido, o Brasil ocupa o quarto lugar no ranking mundial de consumo de material de pedofilia.

Diante de tal situação, é necessária uma análise mais detida acerca desse tópico. O objetivo principal dos pedófilos é envolver as crianças e adolescentes psicologicamente, ou seja, de modo encantador, para conseguir fotos ou vídeos pornográficos, e isso traz uma grande preocupação para as operações policias, a fim de combaterem tal crime.

O Estatuto da Criança e do Adolescente descreve os artigos 240, 241 a 241-D, que tratam da produção e comercialização de cenas pornográficas envolvendo criança ou adolescente. Ademais, a mesma discorre sobre a punição da conduta do agente que reproduziu, armazenou ou expos fotos ou vídeos de materiais pornográficos.

Segundo Ângelo Roberto Ilha da Silva:

> {...} pois há quem pratique o delito de consumo, em suas diversas formas, como trocar, adquirir, possuir, pelo fato de ter essa preferencia sexual, mas há quem pratique o crime por curiosidade, oportunidade, bem como no objetivo de obter ganhos financeiros, havendo organizações criminosas dedicados à produção e venda de material pornográfico envolvendo crianças e adolescentes. (2018. P.89)

Para encontrar os criminosos que praticam esses crimes, são necessários um rastreamento desses computadores que possuem materiais pornográficos para a quebra do sigilo, e assim identificar agente que praticou tal conduta ilícita, vez que, na maioria das vezes cometem de forma anônima.

CAPITULO II – TRATAMENTO LEGAL

O meio virtual e sua constante evolução tecnológica impõe novos desafios aos legisladores para conceituar, tipificar e punir as condutas delituosas praticadas no âmbito virtual. Embora seja uma realidade muito contemporânea, é possível observar a movimentação do Poder Legislativo, com algumas leis em vigência, projetos de leis, com o intuito de combater determinados crimes no ambiente virtual, conforme apresentaremos a seguir.

2.1 – Marco civil da internet

A criação do marco civil da internet se originou para regulamentar questões envolvidas com a internet, estabelecendo princípios, garantias, direitos e deveres que regulam o uso adequado da internet no Brasil. Outrossim, a construção do marco civil foi marcada pela democracia, pois a sociedade participou de forma ativa de todo o processo de criação, tornando assim um ocorrido marcante.

O marco civil da internet é uma lei que pode ser chamada também de “a Constituição da Internet”, pois a sua aprovação permitiu um novo campo para o direito brasileiro, que foi dividida em duas partes, a primeira foi um debate sobre os princípios que orientariam em todo o projeto, e a segunda efetivava tais princípios para a concretização do texto legal.

Nas palavras de Ronaldo Lemos, o marco civil teria que promover a liberdade de expressão, a privacidade, a neutralidade da rede, o direito de acesso a internet, os limites a responsabilidade dos intermediários e a defesa da abertura da rede. (LEMOS, 2014, p. 5)

Deste modo, o marco civil foi um objeto de responsabilidade social, onde qualquer pessoa tinha a possibilidade de expressar a sua opinião sobre o tema em discussão para permitir o fluxo de contribuições técnicas no processo de criação de leis. Ademais, também se levou em consideração as possibilidades de a sociedade contribuir pelas redes sociais, como blogs e twitter.

A lei 12.965 que regula o marco civil da internet foi aprovada como importante conquista democrática e social, entrando em vigor dia 23 de abril de 2014. Deste modo, o marco civil se tornou uma inovação para a metodologia legislativa, um avanço

para uma sociedade cada vez mais digital, gerando um resultado de longos debates e dando respostas para questões de pró-inovação e pró-direitos no âmbito virtual.

O Marco civil da internet se assenta em três pilares, que são: garantia da neutralidade da rede, proteção à privacidade do usuário da Internet, e a garantia da liberdade e expressão. Esses princípios são de suma relevância diante do ambiente virtual, pois há uma preocupação dos dados que são disponibilizados pelos usuários, dos provedores que recebem esses dados, e ainda de não suprimir um direito constitucional diante das regras de proteção. (AKCHAR, 2017)

A garantia da neutralidade da rede é um tema bastante polêmico, mas se diz respeito a preservação dos dados dos usuários que trafegam pela internet. Sua regulamentação está expressa no artigo 9º da lei 12.965/14, onde descreve que quaisquer pacotes de dados devem ser tratados de forma isonômica, sem distinguir o conteúdo, ou seja, esses pacotes não podem ser tratados de forma desigual na rede onde são roteados.

Desta forma, o tratamento isonômico dos pacotes de dados, garante que a internet seja um canal livre para a comunicação, além de preservar a liberdade de escolha dos usuários e da livre concorrência. Assim, sem a neutralidade da rede, os provedores poderiam discriminar alguns conteúdos em função do seu destino e/ou origem, impedindo que chegasse até o aplicativo de acesso do usuário.

Em relação a privacidade dos usuários da internet, está cada vez mais difícil alcançar uma proteção necessária, haja vista que há um grande número de informações pessoais sobre os usuários espalhados pelo mundo a fora, seja ela por espontânea vontade, por necessidade ou condição para o uso da internet.

Salienta-se ainda, que o Marco Civil da Internet, estabelece no seu artigo 3º, inciso II e III da lei, regras concretas sobre a proteção da privacidade dos dados pessoais, logo no art. 7° enumera direitos aos usuários sobre o acesso à internet, e por fim no art. 8° estabelece garantias de privacidade, além de algumas cláusulas contratuais nulas que violam o sigilo das comunicações privadas pela internet.

Ressaltamos que a garantia da liberdade e expressão também está prevista na Constituição Federal em seu artigo 5º, inciso IV, inciso XIV e no artigo 220, que estabelecem, respectivamente a livre a manifestação do pensamento, assegurando a

todos o acesso à informação e resguardado o sigilo da fonte e dentre outras garantias dispostas na Constituição.

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

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

Desta maneira, toda manifestação de opinião exerce impactos sobre os outros, e a liberdade de expressão não abrange qualquer tipo de violência, nem mesmo a coação física ou moral.

Damásio de Jesus e José Antônio Milagre nos ensina que, não é permitido censura na internet, assegurando que a internet é livre e democrática, visto que a garantia da liberdade de expressão tende a sempre prevalecer, desde que não viole direitos de terceiros. (JESUS, MILAGRE, 2014)

2.2 – Lei Carolina Dieckmann

A lei n. 12.737 entrou em vigor no mês de novembro de 2012. O surgimento da lei se deu logo após um acontecimento inesperado envolvendo a atriz, onde várias fotos intimas foram divulgadas ao público, devido a uma invasão de sua privacidade seguida de extorsão. Ademais, na época, debateu-se bastante o tema inclusive em caráter de urgência, cujo resultado culminou na edição da referida Lei.

Auriney Uchôa de Brito, nos ensina que, “para ser legítima a tutela penal é necessária que o bem seja ‘digno’ dessa proteção, e que sua lesão ou ameaça efetivamente mereça uma sanção penal” (2009). No entanto, todas as complicações que envolviam novas condutas no âmbito virtual eram ilegítimas perante o Direito Penal, no tocante a sua punição, e em razão disso, surgiu a Lei nº 12.737/2012.

Tal conflito só teve fim após o episódio citado acima envolvendo a atriz Carolina Dieckmann, pois até então, não havia uma tipificação legal para tutelar a conduta praticada. E com isso, surgiu a Lei n.12.737/12, acrescendo os artigos 154-A e 154-B, do Código Penal que tipificam o crime de invasão de dispositivo de informática, onde o agente comete tal conduta, mediante violação indevida de mecanismo de

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

Por fim, a referida Lei também alterou os artigos 266 e 298 do Código Penal, ajustando-os para o meio cibernético. O artigo 266 teve seu título modificado, passando a se intitular “Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública”. Já no artigo 298 foi acrescido um parágrafo único, que discorre sobre o crime de Falsificação de cartão, onde o legislador equiparou o uso de cartão de credito ou debito ao crime de Falsificação de documento particulares. (BRASIL, 2012)

2.3 – Lei Azeredo

Ainda no ano de 2012, surgiu a Lei nº 12.735, intitulada de “Lei Azeredo”, que teve iniciativa com o projeto de Lei nº 1.999 (PL 84/99). Tal norma visava a tipificação de condutas realizadas por meio do uso de sistema eletrônico, digital ou similares e que fossem praticadas contra sistemas informatizados. (BRASIL, 2012)

Posto isto, a referida norma foi sancionada em um momento onde ocorreram diversos crimes cibernéticos e, em razão disso, houve uma necessidade de elaboração de leis punitivas para condutas realizadas através da internet, como menciona Delmanto:

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

CAPITULO III – MEIOS DE COMBATE

Crimes informáticos é uma realidade vivenciada por milhões de usuários, haja vista que o número de acessos aumenta diariamente de forma inesperada, tornando-se a internet um território sem limites, gerando assim, uma certa complexidade para a produção de provas e da competência para julgar acerca desses crimes. Posto isso, apresentaremos com detalhe os meios de produção de prova e a competência dos tribunais para julgar os crimes informáticos, a seguir.

3.1 – Produção de provas

O Código de Processo Penal, no artigo 155, estabelece que a produção de provas é o ato de reconstruir um fato já que já aconteceu, para obter a verdadeira situação delituosa, o que gera de certa forma, uma contribuição para o convencimento do fato, se ele existe ou inexiste para o juiz. Posto isso, a produção de provas é um meio essencial para a fundamentação justa de uma decisão judicial.

Deste modo, as provas, para serem incluídas no processo, precisam ser integras e verdadeiras, servindo assim para a reconstituição do fato ocorrido, uma vez que o juiz é um desconhecido perante o ocorrido, e somente irá conhecer os verdadeiros fatos através das provas, e assim construir uma convicção ideal.

Mediante isso, as provas que não são notórias, precisam ser provadas, para que se tornem válidas e justificadas pela lei, ou seja, expressa pelo ordenamento jurídico, o que torna um meio para discutir questões controversas sobre a realização do fato, colocando assim características para a prova não ser negada perante o Juiz.

Ainda existem as provas ilícitas previstas no Código de Processo Penal, pelo art. 157, ou seja, aquelas que são contraditas as normas de direito material e constitucional, portanto elas não são aceitas no processo, como por exemplo, a prática de crime de tortura para conseguir alguma informação.

E ainda, os artigos 231 e 232 ambos do referido código, regulamentam acerca dos meios de provas e de algumas possibilidades da utilização de documentos públicos ou particulares, que poderão ser apresentados em qualquer fase do processo, não especificando sobres os documentos por meio eletrônico.

No que se refere a meios e obtenção de provas a uma diferença entre ambas, onde o meio de prova oferece ao juiz meios de conhecimento, da origem do crime,

cujos resultados influenciam na decisão, por exemplo, as provas testemunhais, etc. Em contrapartida, obtenção de provas, são instrumentos que permitem chegar-se à prova, ou seja, servem para adquirir objetos materiais, ou declaração de forca probatória, exemplo, interceptações telefônicas, busca e apreensão, etc. (LOPES JÚNIOR,2019, p.424)

Posto isto, os crimes cibernéticos se limitam na obtenção de provas, haja vista, que na maioria das vezes, os criminosos agem de forma anônima, sem deixar quaisquer vestígios, ou seja, agem de forma silenciosa, através do uso de ferramentas tecnológicas modernas.

Com isso, os profissionais se deparam com uma grande dificuldade, onde os mesmos se encontram despreparados para determinada função, além de não ter ferramentas investigativas adequadas capazes de identificar os agentes criminosos atrás de tais de crimes cometidos.

Desse modo, Alessandro Gonçalves Barreto, diz:

> "Muito da dificuldade encontrada no combate ao cibercrime advém da própria natureza do meio onde ocorre uma parte dos atos executórios do delito: o ciberespaço. Este pode ser conceituado como 'o espaço indefinido onde os indivíduos transacionam e se comunicam', ou ainda, 'o lugar entre os lugares'... É fato, infelizmente que o poder público não consegue reconhecer a potencialidade delitiva de novas tecnologias. A resposta dada pelo aparato policial e judicial está muito aquém do mínimo necessário para uma repressão adequada."

Outra dificuldade no meio de produção de provas é a perícia, pois os peritos precisam de uma autorização do ente competente para que possam investigar os criminosos para obterem informações do IP. Sendo assim, essa autorização tem que ser concedida da maneira mais rápida possível, caso ao contrário corre-se o risco de se perder todo o trabalho e tempo de investigação, haja, vista que os criminosos não armazenam informações por longo tempo.

Por fim, é imprescindível o desenvolvimento de uma capacitação avançada para os agentes, como, laboratórios, equipamentos modernos, para aquisição nos computadores de programas que consigam identificar e localizar os suspeitos, já que o potencial dos delituosos vem aumentando de forma significativa.

3.2 – Competência

Para a compreensão do conceito de competência, é necessário entendermos primeiro o que é jurisdição. Com isso, a jurisdição, é o poder que o Estado tem diante da sua soberania, para aplicar lei ao caso concreto, com o objetivo de solucionar os conflitos de interesses. Em contrapartida, a competência delimita a jurisdição, em outras palavras, define o espaço da aplicação de cada jurisdição.

Nesse sentido, Theodoro Júnior, diz que:

> "Se todos os juízes tem jurisdição, nem todos, porém, se apresentam com competência para conhecer e julgar determinado litígio. Só o Juiz competente tem legitimidade para fazê-lo."

Dessa maneira, não existe apenas um juiz para julgar todos os processos do país, e sim, existe uma competência para limitação dos órgãos que poderão aplicar e julgar o direito em determinada matéria de fato, ou seja, todos os juízes possuem uma jurisdição especifica, mas depende da competência para poder julgar.

Guilherme Nucci, define competência como:

> Trata-se da delimitação da jurisdição, ou seja, o espaço dentro do qual pode determinada autoridade judiciária aplicar o direito aos litígios que lhe forem apresentados, compondo-os. O Supremo Tribunal Federal tem competência para exercer sua jurisdição em todo o Brasil, embora, quanto à matéria, termine circunscrito a determinados assuntos. Não pode, por exemplo, o Ministro homologar uma separação consensual de casal proveniente de qualquer parte do país, embora possa, conforme o caso, apreciar um habeas corpus de pessoa presa em qualquer ponto do território brasileiro. O juiz de uma pequena cidade pode tanto homologar a separação consensual de um casal residente no mesmo local, quanto analisar uma prisão ilegal realizada por autoridade policial da sua Comarca. Não pode, no entanto, julgar casos pertinentes à Comarca vizinha. (2016, p.241)

De acordo com o Superior Tribunal de Justiça (STJ), a competência para julgar crimes informáticos é o lugar de onde partiu o ato delituoso, ou seja, o território que ocorreu a ação de fato. O Código Penal traz em seu artigo 6º, uma teoria ampla, chamada de "teoria da ubiquidade", através dela o lugar do crime, é onde *ocorreu a ação ou omissão, bem como onde produziu ou deveria produzir resultado*.

Para que essa teoria seja aplicada é necessário analisar a ação ou omissão do agente, haja vista que a conduta não pode ser diretamente lesiva, mas precisa ter deixado vestígios para que ocorresse de tal forma, ou até mesmo a instalação de um programa de inteligência *hard*, para a realização dessas condutas.

CONSIDERAÇÕES FINAIS

O presente artigo abordou as diferentes concepções de cibercrimes, ademais, o tema trabalhado é extremamente relevante, pois é a realidade vivida no dia a dia de milhões de pessoas que vem sofrendo ataques, chantagens, ameaças, perseguições dentre outras práticas que surgem juntamente com o avanço tecnológico na sociedade atual.

É importante ressalvar que conforme o artigo 5º, inciso IV da Constituição Federal, é livre a manifestação de pensamentos, porém é vedado o anonimato que é um meio indispensável para que ocorra um crime informático. Ainda, a Lei do Marco Civil, que protege os usuários para não terem sua intimidade e vida privada expostas a terceiros por meio de dispositivos informáticos sem o seu livre consentimento, o que chamamos de Direito de privacidade.

Entretanto, temos outras legislações vigentes que vigora e pune os crimes informáticos, que são elas a Lei n.12.737/12, acrescendo os artigos 154-A e 154-B, do Código Penal que tipificam o crime de invasão de dispositivo de informática, a Lei nº 12.735/12 que visa a tipificação de condutas realizadas por meio do uso de sistema eletrônico, digital ou similares e, a lei 12.965/14 que regula o Marco Civil da Internet estabelecendo princípios, garantias, direitos e deveres.

Ademais, observa-se que há uma dificuldade para o Poder Judiciário nos meios de produção de provas, diante das deficiências de ferramentas capazes de fazer a identificação de autoria, para saber quem está por trás desses crimes, uma vez que os criminosos utilizam do anonimato, prejudicando ainda mais o trabalho das pericias, visto que, os dados armazenados nos IP’s são de pouco tempo.

Por fim, as novas formas tecnológicas, ou seja, as novas modalidades de aplicativos que vem surgindo, trazendo consigo diversas funções que estas fornecem aos usuários, modificam e trazem algumas consequências para a sociedade em si. O que torna as redes sociais com menos privacidade e mais vulnerabilidade dos usuários, com isso, é de suma importância a conscientização do risco que o uso inadequado da internet pode causar problemas na vida de bilhões de usuário, por isso é sempre bom utilizar as redes sociais com sabedoria.

CYBERCRIMES

The vulnerability of users

This article sought to analyze the cyber crimes practiced in Brazil, correlating the legal treatment, as well as the means of combat. To this end, the work aimed to address the different conceptions of cybercrimes, the most vulnerable types of cybercrimes, the application of norms to these crimes, in addition, it identified the means of effective combat, the competence to judge certain crimes and decisions of the courts already existing in the legal system on the subject. The study was based on the reading of articles and scientific works, with special mention to certain authors such as Fernando Capez, Marco Antônio Zanellato, Wanderson Castilho, Jose Antônio Milagre de Oliveira, Pedro Rama, etc. The proposal was to divide the present study into three chapters. The first chapter deals with the history of cybercrimes, as well as conceptualizes and classifies the types of cybercrimes. The second chapter presents the legal treatments on the subject and, finally, the third chapter discusses the means of combating cyber crimes.

Keywords: Crimes. cybernetics. Internet. Species. Legislation.

REFERÊNCIAS

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 19 Set. 2021

BRASIL. **Decreto-Lei no 2.848, de 7 de dezembro de 1940 (Código Penal).** Disponível em: http://www.planalto.gov.br/ccivil_03/decreto- lei/del2848compilado.htm. Acesso em: 22. Set. 2021

BRASIL. **DECRETO-LEI Nº 3.689, DE 3 DE OUTUBRO DE 1941.** Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm. Acesso em: 22. Set. 2021

BRASIL. **Lei n° 12737, de 30 de novembro de 2012.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 04. Out. 2021

BRASIL. **Lei n° 12735, de 30 de novembro de 2012.** Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 04. Out. 2021

BRASIL. **Lei n° 8.069, de 13 de julho de 1990 . Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Planalto.gov.br.** Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 26. Nov. 2021

BRASIL. **A Declaração dos Direitos do Homem e do Cidadão.** Disponível em: https://br.ambafrance.org/A-Declaracao-dos-Direitos-do-Homem-e-do Cidadao#:~:text=estabelecida%20pela%20lei.,Art.,nos%20termos%20previstos%20na%20lei. Acesso em: 29. Nov. 2021

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

Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação - Âmbito Jurídico - Educação jurídica gratuita e de qualidade (ambitojuridico.com.br) GRECO, Rogério. Resumos Gráficos de Direito Penal, Parte Especial – vol III. 7ª. ed
- Niterói, RJ : Impetus, 2012.

SYDOW, Spencer Toth. Curso de Direito Penal Informático, Partes Geral e Especial– 3ª ed – JusPodivm.2022.

AKCHAR, Jamili. Breve análise dos princípios essenciais do Marco Civil da Internet – Lei 12.965/14. Jusbrasil. 2017. Disponível em: https://jamili.jusbrasil.com.br/artigos/435150451/breve-analise-dos principiosessenciais-do-marco-civil-da-internet-lei-12965-

4#:~:text=O%20Marco%20Civil%20da%20Internet,da%20rede%2C%20conforme%20a%20seguir.

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

(ÂNGELO ROBERTO ILHA DA SILVA. *Crimes Cibernéticos.* Editora: Livraria do Advogado)

(BARRETO, Alesandro; KUFA, Karina; SILVA, Marcelo. *Cibercrimes e seus reflexos no direito brasileiro.* 2ª Edição,2021. Editora: Jus Podivm)

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

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

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004, p. 110.

JOSE ANTONIO M MILAGRE DE OLIVEIRA. **Manual de Crimes Informáticos (p. 78).**

https://jus.com.br/artigos/61325/crimes-ciberneticos-e-invasao-de-privacidade-a-luz- da-lei-carolina-dieckmann

https://ambitojuridico.com.br/cadernos/direito-penal/crimes-ciberneticos- consideracoes-sobre-a-criminalidade-na-internet/

G1 > Política - NOTÍCIAS - Brasil é o quarto no ranking da pedofilia, diz PF. **Globo.com.** Disponível em: http://g1.globo.com/Noticias/Politica/0,,MUL747259- 345601,00-BRASIL+E+O+QUARTO+NO+RANKING+DA+PEDOFILIA+DIZ+PF.html.

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

LINS, Bernardo Felipe Estellita. **A evolução da Internet: uma perspectiva histórica**. http://www.belins.eng.br/ac01/papers/aslegis48_art01_hist_internet.pdf

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

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

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

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

THEODORO JÚNIOR, *Humberto. Curso de Direito Processual Civil* - **Teoria geral do direito processual civil e processo de conhecimento. 51**. ed. Rio de Janeiro: Forense. 2010

CAPEZ, Fernando. **Curso de processo penal**. 21ª. Ed. – São Paulo: Saraiva,2014.

Manual de Processo Penal e Execução Penal. 13. ed. Rio de Janeiro: Forense, 2016. Guilherme de Souza Nucci