FACULDADES INTEGRADAS SANTA CRUZ DE CURITIBA

OS CRIMES VIRTUAIS NO BRASIL

Alan Alves

Curitiba/PR

2016

FACULDADES INTEGRADAS SANTA CRUZ DE CURITIBA

OS CRIMES VIRTUAIS NO BRASIL

Monografia apresentada como requisito parcial de Conclusão de Curso para obtenção do Grau de Bacharel em Direito, sob orientação do Prof. Laiza Padilha dos Santos.

Curitiba/PR

2016

OS CRIMES VIRTUAIS NO BRASIL

Trabalho de Conclusão de Curso aprovado como requisito parcial para obtenção do Grau de Bacharel em Direito

_____

LAIZA PADILHA DOS SANTOS

Orientador

_____

CAMILA WITCHMICHEN PENTEADO

Examinador

_____

REGINA ELISEMAR CUSTÓDIO MAIA

Examinador

Curitiba/PR, 06 de Dezembro de 2016

AGRADECIMENTOS

Primeiramente agradecer a Deus por permitir o desenvolvimento do presente trabalho, bem como a conclusão do mesmo.

Agradeço as Faculdades Santa Cruz, principalmente aos Profs. José Antonio Soares, Mirian Moreira da Silva Soares e Hugo Eduardo Meza Pinto, por oportunizar a um outrora menor aprendiz, a encaminhar a conclusão de mais uma graduação através do presente trabalho.

Agradeço ao Prof. Arion Bastos que foi o grande incentivador na busca por novos conhecimentos, principalmente no que toca a área de Direito.

Agradeço a Prof. Laiza Padilha dos Santos por toda a dedicação, paciência, empenho e motivação dada para que pudesse chegar à conclusão do presente trabalho.

Por fim, agradeço a Prof. Gilmara Funes, coordenadora do curso e a todos os Professores do curso que ministraram aula durante os cinco anos e que de alguma forma contribuíram para o meu desenvolvimento intelectual.

DEDICATÓRIA

Dedico o presente trabalho a minha mãe Sra. Maria Laura de Oliveira Alves que sempre esteve ao meu lado durante o curso, dentro suas possibilidades e limites, de alguma forma incentivando e dando apoio necessário, desde sempre, para que pudessem um dia chamar seu filho de “Dourtor”.

Dedico ao meu pai Dinizar Alves (em memória) que durante o desenvolvimento do presente trabalho veio a falecer, mas que sempre foi meu grande ídolo, e que da mesma forma que a minha mãe também incentivou e esteve do meu lado em todos os momentos. Aonde quer que esteja, espero que esteja orgulhoso.

Dedico a minha namorada Ketlin Arnas por estar comigo nesta reta final de curso e ser compreensiva por inúmeros momentos, e que em cada dia de desenvolvimento do trabalho se quer pensou em ficar longe, e sempre que pôde colaborou para o desenvolvimento deste. À Ketlin e a toda a sua família.

Dedico a minha filha Bruna Eliady Carvalho Alves pela compreensão na abdicação de alguns momentos e para que o presente trabalho sirva de inspiração e norteie seus passos principalmente no aspecto educacional.

Por fim, dedico a todos meus amigos, que fazem parte da minha vida e que em algum momento ao longo deste árduo caminho estiveram juntos em todos os momentos.

Esse é o principal ponto da tecnologia.
Por um lado, ela cria um apetite por imortalidade e,
por outro, ameaça extinção universal.
(Don DeLillo)

RESUMO

Os crimes virtuais, tema do presente trabalho, são crimes cometidos através do uso de dispositivos tecnológicos. Eles fazem parte da atual Sociedade da Informação, onde a tecnologia passou a fazer parte do cotidiano das pessoas. Neste sentido passa-se a ter um problema social, e que dá origem ao problema do presente trabalho que são os crimes realizados por meio de dispositivos tecnológicos e a legislação que toca ao tema. A metodologia utilizada é a abordagem do tema crimes virtuais, de forma que se apure a legislação dentro do território nacional, utilizando-se para o desenvolvimento o método como a pesquisa bibliográfica, ou seja, o uso de livros, artigos, monografias e publicações acerca do tema. Estes crimes podem ser divididos em: crimes virtuais próprios, sendo estes os que somente podem ser cometidos através do dispositivo tecnológico, como por exemplo, na conduta prevista de invasão a computador, tipificada pelo art. 154-A que foi fruto da Lei n° 12.737/2012 (Lei Carolina Dieckmann); e crimes virtuais impróprios que são aqueles que se utilizam do computador apenas como meio e que poderiam ser cometidos sem a utilização de dispositivos tecnológicos, como, por exemplo, fraudes, furto, falsidade ideológica, dentro outros. Logo, o objetivo geral do presente trabalho, é a apresentação da tipificação dos crimes virtuais pela legislação brasileira. Como sujeitos destes crimes, têm-se os sujeitos ativos destes tipos de condutas que possuem características ímpares por possuírem conhecimento técnico avançado em tecnologia, já com relação ao sujeito passivo pode ser qualquer pessoa física ou jurídica, de direito público ou privado desde que seja titular do bem jurídico lesado. Por fim, são apresentados alguns procedimentos como a definição da aplicação territorial, ou seja, o local do crime uma vez que são condutas normalmente realizadas em localidade diferente da local onde se obteve o resultado; a definição da jurisdição competente para julgar a conduta criminosa, também complexa por consequência da definição do local do crime e também por casos em que envolvem entes específicos como a União, autarquias e empresas públicas, dentre outros; e a investigação e produção de provas nesta modalidade de crime, a qual tem por objetivo a localização do dispositivo tecnológico inicialmente, apurando informações e evidências através de especialistas na área de tecnologia. Logo em seguida busca-se a identificação do autor da conduta ilícita. Cabe destacar ainda apresentação de algumas decisões dos Tribunais abordando o tema. Como resultados do trabalho pode-se destacar a existência de lei específica que aborda o tema, sendo está á lei 12.737/2012, denominada Lei Carolina Dieckmann, e a adequação de leis já existentes as condutas realizadas por meio de dispositivos tecnológicos; as características específicas dos sujeitos, principalmente os ativos que realizam a conduta e que possuem conhecimentos avançados específicos em tecnologia; a complexidade para a definição do local do crime e da jurisdição competente; e a investigação e produção de provas como procedimentos que envolvem, dentre outros, o agentes de conhecimentos específicos para apuração de informações e evidências no intuito de localizar o dispositivo tecnológico e o autor.

Palavras-chave: Crimes virtuais. Dispositivo tecnológico. Internet. Legislação.

ABSTRACT

The virtual crimes, subject of the present work, crimes are committed through the use of technological devices. They are part of modern Information of society, where technology became part of the daily lives of people. This in sense there's having a social problem, and that gives rise to the problem of present work which are the crimes carried out by means of technological devices and the legislation that touches on the subject. The methodology used is the approach of the theme virtual crimes, so that they established the legislation in the national territory, and to develop the method as the bibliographical research, namely, the use of books, articles, monographs and publications on the subject. These crimes can be divided into: virtual crimes themselves, which are those that can only be committed through the technological device, for example, in the conduct of the invasion, computer for typed. 154-A fruit of the Law n° 12,737/2012 (Carolina Dieckmann Law), and inappropriate electronic crimes that are those who use the computer just as a means and that could be committed without the use of technological devices, such as fraud, theft, misrepresentation, within others. Soon, the general objective of this work is the presentation of the type of crimes by brazilian legislation. As subjects of these crimes have been the subject assets of these types of conduct that have unique characteristics because they have advanced technical knowledge in technology, with respect to the taxpayer can be any person or entity, public or private law as long as it's legal right holder aggrieved. Finally, some procedures are presented as the definition of the territorial application, i.e. the crime scene since they are normally carried out in different locale ducts from where you obtained the result; the definition competent jurisdiction to judge the criminal conduct, also as a result of the definition of the complex crime scene and also for cases involving specific ones like the Union, local authorities and public enterprises, among others; and the research and production of evidence in this form of crime, which aims at the location of technological device initially, with information and evidence through experts in the field of technology. Then there is the author's identification of unlawful conduct. It is worth mentioning still filing some court decisions addressing the theme. As results of the work can highlight the existence of specific law that addresses the issue, and is the law/2012 12,737, named Carolina Dieckmann Law, and the adequacy of existing laws the ducts by means of technological devices; the specific features of the subject, especially the assets that perform and conduct that have advanced knowledge in specific technology; the complexity for the definition of the crime scene and of competent jurisdiction; and the research and production of evidence as proceedings involving, among others, the agents of expertise for verification of information and evidence in order to find the technological device and the author.

Key-Words: virtual Crimes. Technological device. Internet. Legislation.

SUMÁRIO

1 INTRODUÇÃO

Este trabalho destinou-se a exibir como tema os crimes virtuais no Brasil, tendo com área de interesse principalmente o Direito Penal e algumas de suas vertentes, em aspecto geral, que tocam aos ilícitos cometidos por meio de uso da tecnologia.

Neste sentido, a problemática estimuladora ao referente tema enfatizou a forma como o Brasil tipificou, por meio de sua legislação, os crimes virtuais, bem como a punição prevista, e algumas das características deste tipo de crime, uma vez que tendem a ser peculiares.

A justificativa para a apresentação do presente trabalho se motivou por conta de ser tratar de duas áreas de fundamental importância para a sociedade atualmente.

A primeira área é a da tecnologia, a qual atualmente faz parte do cotidiano das pessoas na sociedade, haja vista a forma de abordagem de boa parte da doutrina denominando a sociedade contemporânea como Sociedade da Informação.

Já a segunda área a do direito, diga-se direito penal, é de extrema importância no sentido regular o convívio social entre as pessoas, bem como de impor limites e ditar as regras a serem seguidas dentro da sociedade.

Estes fatores, juntamente com o fato de que os crimes virtuais ser um tema atual e consequentemente ainda novo na esfera jurídica, de forma que ainda tem-se muito a que se desenvolver e somado ao interesse em adquirir conhecimento na área, levaram ao desenvolvimento do presente trabalho.

O objetivo geral do presente trabalho foi apurar os aspectos relevantes aos crimes virtuais especificamente no Brasil, tendo em vista toda a complexidade e particularidade que esta modalidade de crime apresenta, em uma abordagem mais ampla e perfunctória, de forma a proporcionar uma visão do todo acerca do tema.

De forma analítica, como objetivos específicos apresentou-se a tecnologia atual e a sociedade contemporânea; o estudo dos crimes virtuais no Brasil no tocante a: legislação, sujeitos, local do crime, jurisdição e investigação para esta modalidade de crime.

Com relação à metodologia utilizada neste trabalho foi por meio de abordagem dos crimes virtuais em aspecto amplo na atual sociedade, apresentando características e legislação sobre o tema. Posteriormente foi abordado, na delimitação do território brasileiro, expondo como a legislação brasileira vem tratando tal disciplina e os procedimentos realizados. Logo, neste caso o método inicial utilizado foi o método comparativo.

Ainda sobre a metodologia, foi utilizado também o método bibliográfico o qual permitiu que fossem levantadas as bibliografias publicadas que disciplinam sobre o tema, trazendo em forma de livros, publicações como artigos e monografias e ainda sites, doutrinando, legislando ou ainda decidindo acerca do tema. Neste sentido, necessária foi a pesquisa bibliográfica, através de bibliografias e legislação vigente, visualizando como foram tratados, até o presente momento, os crimes virtuais no Brasil.

As hipóteses previstas eram a exposição no trabalho das leis e das doutrinas pesquisadas existentes acerca do tema, e a previsão de mais leis específicas referentes ao tema além das já existentes, de forma que pudessem complementar o ordenamento jurídico brasileiro no que toca a matéria de crimes virtuais.

Isto posto, o trabalho abordou o tema abarcando os seguintes aspectos: os conceitos atuais de tecnologia e seus respectivos dispositivos tecnológicos, sendo estes os mais comuns e atualmente abordados pela doutrina; os conceitos de crimes virtuais apresentados pela doutrina, bem como as classificações apresentadas; a tipificação dos crimes virtuais mais comuns no contexto atual da sociedade de acordo com a doutrina e o ordenamento jurídico brasileiro; os sujeitos desta modalidade no que toca aos sujeitos ativos e passivos, bem como no caso dos sujeitos ativos as suas especificidades; o local do crime, principalmente me sua definição; a investigação em uma abordagem mais técnica e a jurisdição no que toca a competência.

O primeiro capítulo ficou por conta da Introdução, ou seja, a apresentação do conteúdo do trabalho de forma sintética, bem como a forma como desenvolveu-se o mesmo.

Já o segundo capítulo apresentou conceitos contemporâneos e relevantes, e respectivas características sobre a sociedade atual, também denominada no presente trabalho como "Sociedade da Informação", e a tecnologia

por meio de seus dispositivos os quais fazem parte do cotidiano de toda a sociedade.

No terceiro capítulo foram abordados conceitos básicos do Direito Penal em uma visão da doutrina clássica. Em seguida, apresentou-se as possíveis nomenclaturas utilizadas para os crimes virtuais e os conceitos disciplinados por doutrinadores especialistas no tema.

O quarto capítulo trouxe a classificação dos crimes virtuais, a qual divide este tipo de crime como próprio ou impróprio. Neste sentido, buscou-se apresentar o conceito de cada crime, a tipificação atual brasileira que toca ao tema, de acordo com o que a doutrina apresentou e classificou, e ainda algumas decisões do Poder Judiciário sobre o tema.

No quinto capítulo, buscou-se apresentar os sujeitos do crime, sendo estes o sujeito ativo e o sujeito passivo. Cabe ressaltar que no tocante ao sujeito ativo dos crimes virtuais, abordou-se a forma específica que os doutrinadores apresentaram para as características das pessoas que cometem as condutas virtuais ilícitas.

Os procedimentos realizados para o crimes virtuais foi o tema do sexto capítulo e último capítulo, descrevendo como são realizados alguns procedimentos como a definição do local do crime, a investigação e provas e ainda a definição de competência para esta modalidade de crime.

No tocante ao local do crime, foram apresentadas particularidades para apuração do território, tendo em vista que os crimes virtuais são cometidos por meio de dispositivos tecnológicos e em boa parte cometidos a distancia, o que pode impor obstáculos à definição do local.

Quanto à investigação e provas, enfatizou-se o aspecto técnico tecnológico como tema, onde buscou-se abordar a identificação e localização do dispositivo tecnológico de onde partiu a conduta criminosa.

Por fim, com relação a definição de competência visou-se apresentar a quem compete o julgamento de ilícitos cometidos virtualmente, ou seja, qual a jurisdição competente para julgar os crimes virtuais.

2 A SOCIEDADE DA INFORMAÇÃO E OS DISPOSITIVOS TECNOLOGICOS

A popularização dos dispositivos tecnológicos bem como da Internet, por conta de toda a globalização e evolução tecnológica, transformou a vida das pessoas, influenciando diretamente no cotidiano da sociedade como um todo.

Destarte, vive-se hoje o que é chamada por grande parte da doutrina que aborda o tema, como a Sociedade da Informação, conforme apresentado a seguir.

2.1 SOCIEDADE DA INFORMAÇÃO

O termo “sociedade da informação” passou a ser utilizado como substituto para o termo de “sociedade pós-industrial” em consequência da realidade de transformação no tocante ao avanço tecnológico e seu impacto perante as organizações. (WERTHEIN, 2000, p.71)

A sociedade da informação tem início a partir da Revolução Industrial a qual proporcionou uma série de inovações tecnológicas com reflexos econômicos e sociais por todo o mundo, influenciando diretamente na substituição da força humana pela máquina, e no desenvolvimento e disseminação de áreas como elétrica, física e química, as quais forneceram elementos de extrema importância para o surgimento da tecnologia. (CRESPO, 2011, p.32)

Esta nova sociedade, da qual se vive nos dias de hoje, traz consigo, por conta dos mais profundos avanços tecnológicos, um novo conceito de vida e organização em sociedade, refletindo nas mais diversas relações sociais como, por exemplo: a produção, uso da informação, mercado, geração de conhecimento, dentre outras. (FIORILLO;CONTE, 2016, p.18)

A partir da década de 90 desenvolve-se a sociedade da informação onde é dada importância significativa aos bens imateriais, como no caso da propriedade intelectual, segredo industrial e depósitos de dinheiro, dentre outros.

Isto se dá por conta da convergência entre informática e telecomunicações, da popularização da internet. (CRESPO, 2011, p.32)

A internet e as tecnologias da informação passam a ter papel fundamental na Sociedade da Informação, pois refletem diretamente na realidade jurídica, trazendo uma nova forma de apreciar os velhos direitos como à informação, à comunicação, à liberdade de expressão e à privacidade. (FIORILLO;CONTE, 2016, p.16)

Estes direitos são previsto pelo artigo 5º da Constituição Federal, o qual versa por meio do inciso IV o direito à liberdade de expressão, disciplinando que “é livre a manifestação do pensamento, sendo vedado o anonimato”; do inciso IX o qual se refere ao direito à comunicação, versando que “é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença”; e por fim o inciso XIV que prevê o direito a informação e a privacidade expondo que “é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional”.

Como consequência do desenvolvimento tecnológico, a Globalização também surge como fator de grande influencia na Sociedade da Informação por conta da evolução social apresentada e traz uma nova interpretação para espaço, não sendo este mais limitado fisicamente, ou seja, o progresso tecnológico reduz o planeta a uma aldeia, aonde qualquer um estabelece comunicação com o outro, passando o mundo a ficar interligado. (CRESPO, 2011, p.36)

Destarte, o avanço tecnológico na comunicação e a globalização sempre tiveram como um de seus objetivos permitirem a criação de uma "Aldeia global", ou seja, a internet no sentido de ser onde as pessoas de todo mundo se comunicam entre si de forma instantânea e onde todos têm o acesso simultaneamente às informações. (PINHEIRO; 2013, s.p.)

Importante ressaltar ainda que o momento social atual não se restringe apenas a utilização de computadores em atividades do cotidiano. As revoluções ocorridas na Sociedade da Informação remodelam conceitos na sociedade, bem como nas relações humanas e em ramos sociais, econômicos e culturais. (FIORILLO;CONTE, 2016, p.18)

Em contrapartida, como ônus da evolução da internet e dos dispositivos tecnológicos, uma vez que estes passam a ter interferência direta nas relações sociais pacíficas, também possibilitam algumas práticas socialmente

desagradáveis e indesejadas, colocando em risco inclusive bens que outrora não tinham relevância para o direito. (FIORILLO;CONTE, 2016, p.16)

Logo, o avanço tecnológico traz consigo, o acompanhamento das condutas criminosas que passam a ser realizadas por meio de dispositivos tecnológicos, ou seja, formas de impor e controlar futuras ações humanas, o que pode influenciar direta ou indiretamente também na prática de condutas criminosas. (CRESPO, 2011, p.32-36)

Neste sentido, surgem os crimes virtuais como uma das espécies do ônus gerados por conta dos avanços tecnológicos, ou ainda como parte dos riscos da modernização e de dimensão social principalmente, uma vez que o uso indevido da tecnologia cotidiana pode trazer sérias ameaças, dentre elas a delinquência informática como um fenômeno social. (CRESPO, 2011, p.36)

A globalização e os avanços tecnológicos, assim como exigem das pessoas e da sociedade a alfabetização tecnológica, também exigem que o pensamento jurídico acompanhe tal evolução de modo que se possa a aplicar as normas de acordo com os contextos impostos. (PINHEIRO; 2013, s.p.)

Neste diapasão, Fiorillo e Conte (2016, p.16) disciplina que:

> O direito deve se adequar à nova realidade, sob pena de perder seu verdadeiro papel, qual seja disciplinar as relações sociais e impor normas de conduta. Assim o binômio Direito e Internet não constitui fenômeno passageiro. Trata-se de uma realidade ainda pouco explorada, mas que deve ser analisada sob todos os campos das ciências jurídicas, afim de garantir novos direitos fundamentais, bem como a efetivação dos já existentes.

Logo, como o direito é mutação e o virtual é mutável, é importante para toda esta nova sociedade ou Sociedade da Informação, que ambos os sistemas estejam sincronizados para que, além de trazer mudanças profundas, possam acompanha-las principalmente no aspecto jurídico. (OLIVEIRA, 2011, s.p.)

2.2 TECNOLOGIA E DISPOSITIVOS TECNOLÓGICOS

Desde os primórdios até os dias atuais o homem e a sociedade vêm em ininterrupta e constante evolução, fato este que proporciona sempre novas

demandas e exigências sociais para as suas necessidades, as quais de tempos em tempos tendem criar-se ou renovar-se.

Para que se possa atender a uma destas demandas e exigências sociais de forma eficiente e eficaz, em determinados momentos da história, surge a tecnologia, conforme disciplina Reis, (2009, s.p.) “Na verdade, foi a engenhosidade humana, em todos os tempos, que deu origem às mais diferenciadas tecnologias”.

Ainda neste sentido, cabe ressaltar que:

> Cada sociedade cria, recria, pensa, repensa, deseja e age sobre o mundo através da tecnologia e de outros sistemas simbólicos. A tecnologia é impensável sem admitir a relação entre o homem e a sociedade. (LION, 1997, [s.d.] apud VERASZTO, [s.d.], p.77)

Para Chagas (2008, p.4329), “tecnologia é um conjunto de métodos, técnicas e conhecimentos aplicados a resolução de problemas, produção de bens e serviços relacionados ás necessidades humanas”.

Destarte Lion (1997, p.77) complementa e conceitua a tecnologia como:

> [...] um conjunto de saberes inerentes ao desenvolvimento e concepção dos instrumentos (artefatos, sistemas, processos e ambientes) criados pelo homem através da história para satisfazer suas necessidades e requerimentos pessoais e coletivos.

Atualmente a tecnologia tem grande influência na vida do homem e consequentemente na sociedade da informação, haja vista o papel que cumprem os computadores e demais dispositivos tecnológicos, os quais influenciam de forma significativa em seus respectivos cotidianos, conforme cita Silveira e Bazzo (2005, s.p.)

> Vivemos num mundo em que a tecnologia representa o modo de vida da sociedade atual, na qual a cibernética, a automação, a engenharia genética, a computação eletrônica são alguns dos ícones que da sociedade tecnológica que nos envolve diariamente.

Para Cardoso (2006, s.p.) “Hoje presenciamos um cenário de constante inovação, com máquinas cada vez mais modernas, e que mais bem atendem às necessidades de uma sociedade amplamente aderida ao advento da tecnologia”.

Logo, fica claro que a tecnologia passou a fazer parte do dia-a-dia do homem contemporâneo e que o cenário tecnológico atual é de desenvolvimento e

evolução constante, acompanhando as necessidades do homem e da sociedade, bem como ditando tendências à vida humana individual ou coletiva.

Neste diapasão é que a sociedade da informação apresenta diversas formas de dispositivos tecnológicos para que as pessoas possam acompanhar evolução tecnológica acelerada, principalmente no tocante ao desenvolvimento dos meios de informação e comunicação. (SILVA, 2015, p.19)

Os dispositivos tecnológicos são instrumentos tecnológicos que tornaram-se populares perante a sociedade, como por exemplo os dispositivos móveis, dentre eles tablets, smartphones, celulares, e que seus respectivos potenciais permitem que realizem atividades como se fora computadores pessoais, ou seja, possibilitam as pessoas navegar pela internet, acessar o seu Internet Banking, acessar e-mails ou ainda acessar redes sociais. (CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL, 2012, p.107)

A seguir é possível acompanhar alguns dos mais comuns dispositivos tecnológicos que fazem parte atualmente da Sociedade da Informação, bem como seus respectivos conceitos e características.

2.2.1 Informática

A evolução tecnológica tem importante papel ao longo da história e impacta até os dias atuais e nas mais variadas áreas, haja vista a Revolução Industrial, onde a tecnologia deu vida às máquinas para que se tivesse a partir de determinado momento as produções em largas escalas e a automação dos processos industriais. Uma evolução que se mantêm e se aprimora a cada dia. (CRESPO, 2011, p.28)

Não diferente, a tecnologia também evoluiu de forma a atingir a área das informações. Neste diapasão é dado origem a informática.

A informática representa uma forma de automação da informação, que utiliza como meio dispositivos tecnológicos para automatizar informações. (KOZAC, 2002, p.1)

Para Kozac (2002, p.1) a informática tem o seguinte significado:

> Informática pode ser considerada como significando “informação automática”, ou seja, a utilização de métodos e técnicas no tratamento automático da informação. Para tal, é preciso uma ferramenta adequada: o computador eletrônico.

Neste mesmo sentido, e complementando o conceito anterior de forma a relacionar com a automação das tarefas na sociedade, entende Willrich (s.d; s.p.) que

> A informática engloba toda atividade relacionada ao desenvolvimento e uso dos computadores que permitam aprimorar e automatizar tarefas em qualquer área de atuação da sociedade

Já Marçula (2008, p.46) destaca a informática como estudo do tratamento de informação através de algum tipo de dispositivo tecnológico onde o objetivo principal é “o tratamento da informação usando como ferramenta os recursos de sistemas de computação, ou seja, o computador e outros recursos ligados a ele”.

Com toda a evolução e avanço, a informática passou a ter papel fundamental nos dias atuais, implicando diretamente nos padrões sociais e no comportamento do homem contemporâneo, logo:

> Os avanços das telecomunicações e da informática nos últimos anos revolucionaram a sociedade contemporânea, criaram novos padrões sociais, moldaram novos comportamentos, redirecionaram a economia e deram um impulso definitivo à globalização. (OLIVEIRA, [s.d.], [s.p.] apud ROVER & WINTER, 2002, p.75)

Atualmente a informática tem um papel importante para todas as atividades do mundo moderno, onde praticamente todos os processos, salvo algumas raras exceções, estão automatizados através de recursos informáticos. Logo a informática supera os estágios de tendência e realidade, tornando-se uma necessidade para que se possa acompanhar a evolução da sociedade e fazer parte da vida do homem contemporâneo.

2.2.2 Computador

O computador é o principal instrumento da informática que surge como um meio de contribuição direta ao nosso cotidiano, impactando de forma à agilizar as tarefas que antes eram realizadas em longo tempo, ou seja reduzindo o tempo das atividades e proporcionando, em conjunto com outras tecnologias, uma maior velocidade nas informações e na comunicação entre pessoas, e também refletindo na sociedade da informação como um todo.

Destarte, o que antes demorava longos espaços de tempos para se conhecer ou para desenvolver agora acontece imediatamente, ou seja, de forma instantânea, como salienta Kozak (2002, p. 1) "o computador é uma máquina que processa dados, orientada por um conjunto de instruções e destinada a produzir resultados completos, com um mínimo de intervenção humana".

Neste mesmo sentido, Viana (1996, p. 26) define o computador como "instrumento físico usado para viabilizar ideias apresentadas pela informática".

Para Marçula (2008, p.49) computador é "uma máquina que recebe e trabalha os dados de maneira a obter um resultado".

Complementa Marçula (2008, p.49) conceituando o computador como "um sistema que tem determinados componentes que, atuando em conjunto permitem que ele realize tarefas que foram especificadas. Este sistema é composto, basicamente, de dois elementos, hardware e software".

O computador ainda pode ser definido da seguinte forma:

> O computador é uma máquina que pode ser programada para aceitar dados (entrada), transformá-los em informação (saída) útil e armazená-los (em um dispositivo de armazenamento secundário) para proteção ou reutilização. O processamento de entrada para saída é conduzido pelo software, mas realizado pelo hardware. (KUROSE, 2003, p.12)

Por fim, Capron (2004, p.49) sintetiza de forma técnica e objetiva o conceito de computador. Para ele computador "é um sistema integrado, composto de hardware e software".

Logo, o computador tem importante papel para a automação das informações, pois é por meio do mesmo que são operacionalizadas as atividades afim de obter-se os resultados no menor tempo possível.

2.2.2.1 Hardware e Software

Como citado anteriormente, o funcionamento do computador deve-se a dois componentes basicamente: o hardware e o software.

Além deste dois componentes, deve haver a interação humana para que possa ser feito o envio do comando. Tão logo o envio do comando é realizado, o computador recebe e processa o dado, transformando-o e retornando-o como a informação.

Neste sentido Kurose (2003, p.12) ressalta que:

> o equipamento de um computador denomina-se hardware. Um conjunto de instruções denominada software diz ao computador o que fazer. As pessoas entretanto são o componente mais importante do computador. Elas que usam o poder do computador para algum propósito.

No tocante ao hardware, Viana (1996, p. 25) conceitua o hardware como “toda espécie de dispositivo físico que componha o computador”.

Ainda para Viana (1996, p.25), “o hardware é, sem qualquer dúvida, uma parte fundamental de qualquer computador. Contudo, a sua pura e simples existência não é suficiente para ter alguma utilidade”.

Neste sentido, Capron (2004, p. 49) sintetiza o conceito de hardware destacando que “hardware é a parte física do computador, ou seja, o próprio computador e todos os dispositivos ligados a ele (periféricos)”.

A definição de Viana (1996, p.25) simplifica extremamente os conceitos da seguinte forma: “hardware é computador, software é programa”.

Já o software é o meio por onde se faz a utilização do hardware, ou seja, o software é que possibilita o funcionamento do hardware.

Para Beck (1993, p.2), o qual denomina o software como “software básico”, “os softwares básicos têm como objetivo possibilitar a operação e o uso computador”.

De forma um pouco mais analítica Pressman (1995, p.12) define o software de três outras formas que se complementam:

> Software é: (1) instruções (programas de computador) que, quando executadas, produzem a função e o desempenho desejados; (2) estruturas

> de dados que possibilitam que os programas manipulem adequadamente a informação; e (3) documentos que descrevem a operação e o uso dos programas.

Logo, fica claro que o hardware e o software são os componentes mais importantes para o computador, pois sem eles não seria possível o funcionamento do computador, entretanto a interação humana é que determina a forma como será utilizada a tecnologia.

2.2.3 Dispositivos Tecnológicos Móveis

Os dispositivos de tecnologias móveis são hardwares derivados dos computadores tradicionais e que utilizam-se dos softwares em atividades como a viabilização da interação do usuário com o equipamento, o armazenamento de dados e o acesso aos mesmos localizados no próprio equipamento ou através de conexão em redes e internet.

Com toda a evolução tecnológica e da sociedade da informação, o surgimento de novas necessidades ficam cada vez mais explícitos. Uma destas necessidades é o uso da tecnologia, em conjunto com a possibilidade de mobilidade do homem contemporâneo.

Neste sentido, Taurion (2002, p.13) ressalta que “a nova sociedade do conhecimento é baseada em mobilidade e flexibilidade”.

Complementa ainda Taurion (2002, p.13) enfatizando que “serviços e informações devem se mover para onde forem necessários e não o contrário, o usuário ou cliente indo até a informação e o serviço”.

Nas últimas décadas houve uma grande progressão do avanço tecnológico, surgindo variações das tecnologias já existentes. Os computadores tornaram-se móveis e ganharam outras versões compactas como os notebooks, palmtop e outros; os telefones que outrora tinham a utilidade de apenas ligação de locais fixos passaram a ter a mobilidade em um primeiro momento através da telefonia celular e em seguida agregado o acesso a informações, dando origem aos atuais smartphones que na visão de Benfica (2016, s.p.) “é um telefone celular com muitas funções”:

Destarte, salienta-se que:

> Atualmente podemos realizar varias funções e atividades através de um computador móvel ou através de um celular móvel. Tanto os computadores cada vez mais leves e acessíveis, como também as novas tecnologias móveis como os celulares, também muito conhecidos como Smartphones que também possuem um sistema operacional, vários aplicativos para desenvolvimento de atividades pessoas e profissionais e tem acesso a internet a qualquer lugar que esteja e tenha disponibilidade de acesso com a internet, podemos definir os Smartphones como os computadores de mão. (PORTAL EDUCAÇÂO, 2014, s.p.)

Logo, pode-se expor que tanto os computadores móveis quanto os celulares e smartphones possibilitam as pessoas a acessarem a internet e aplicativos, sendo estes softwares existentes no dispositivo, de qualquer local que seja e em consequência permitindo que realizem suas atividades onde quer que estejam.

Acompanhando todo a evolução dos equipamentos, ganhou força também a internet móvel, a qual surgiu com o objetivo de atender a demanda de mobilidade, ou seja, do uso dos equipamentos tecnológicos móveis como expõe Taurion (2002, p.2) “O potencial da internet móvel é claro: criar facilidades de acesso aos recursos da internet, de qualquer lugar e a qualquer momento”.

Ainda para Taurion (2002, s.p.) a definição de internet móvel é abordada como “o uso de tecnologias de comunicação sem fio (wireless) para acesso a informações e aplicações web a partir de dispositivos móveis, como celulares ou handhelds”.

2.2.4 Redes e Dados

O surgimento do computador é um grande aliado para operacionalizar atividades que demandariam um grande esforço humano. (TANENBAUM, 2003, p. 2)

Pensando em otimizar a operacionalização das atividades surge a ideia de colocar mais que um único computador a favor da mão-de-obra. Logo surgem a redes de computadores, como cita Tanenbaum (2003, p. 2):

> O velho modelo de um único computador atendendo a todas as necessidades computacionais da organização foi substituído pelas chamadas redes de computadores, nas quais os trabalhos são realizados por um grande número de computadores separados, mas interconectados.

Logo, percebe-se que a interconexão de computadores pode ser utilizada não somente para unir esforços de vários computadores a favor de uma atividade específica, mas também para a comunicação entre eles com a possibilidade de troca de informação, com o seguinte conceito:

> Rede de computadores é um conjunto de equipamentos interligados de maneira a trocarem informações e compartilharem recursos, como arquivos de dados gravados, impressoras, modems, softwares e outros equipamentos. . (ALENCAR, [s.d.], [s.p.] apud SOUZA, 1999, [s.p.])

Neste sentido, Tanenbaum (2003, p. 2) discorre sobre a forma de conexão entre os computadores onde “a conexão não precisa ser feita por um fio de cobre; também podem ser usadas fibras ópticas, microondas, ondas de infravermelho e satélites de comunicações”.

Destarte, a rede de computadores é uma forma de comunicação onde conectam-se dois ou mais computadores fisicamente através de cabos, fibra óptica, sinal de rádio ou outro equipamento, para compartilhar documentos, sistemas, banco de dados, impressoras, planilhas e acesso a internet dentre outros recursos. (IESDE, 2015, s.p.)

Com a interconexão entre os computadores, chega-se a conclusão que a comunicação entre eles permite também a troca de dados realizando assim a comunicação de dados.

Para Forouzan (2008, p.4) comunicação de dados “são as trocas de dados entre dois dispositivos por intermédio de algum tipo de meio de transmissão, como um cabo condutor formado por fios”.

Para Viana (1996, p. 8) dado é “a representação física de um evento” ou ainda “uma representação através de um meio físico para possibilitar posterior utilização”.

Já para Forouzan (2008, p.4) “A palavra dados se refere a informações apresentadas em qualquer forma que seja acordada entre as partes que criam e usam dados”.

Por fim, ressalta-se que a rede de computadores basicamente tem como função principal a comunicação de dados para que possa haver a troca de informações.

2.2.5 Internet

A Internet surge na década de 60, através de pesquisas acadêmicas apoiadas pelo Departamento de Defesa norte-americano, através da Advanced Research Projects Agency (ARPA), com o objetivo de compartilhar informações para que seus componentes pudessem acessá-las em qualquer lugar. (CRESPO, 2011, p.30)

O sistema veio a crescer e logo estava criada uma rede onde tinha-se um ambiente aberto e de possível acesso as mensagens e informações distribuídas para que as pessoas envolvidas pudessem acessá-las. (CRESPO, 2011, p.30)

Em seguida, há uma expansão da rede dentro mesmo do Departamento de Defesa dos EUA, o que gerou interesse de demais departamentos governamentais para a utilização da rede, bem como a possibilidade de distribuição da rede para a sociedade civil, diga-se a população acadêmica. (WENDT;JORGE, 2012, p.6-7)

A década de 90 é marcante pelo fenômeno da globalização e seus reflexos perante a sociedade e na expansão daquilo que já era chamada como rede mundial, haja vista seu alcance por todo o território mundial, conectando pessoas de todo o planeta em um curto espaço de tempo para a comunicação e sem limitação para a diversidade de temas. (FIORILLO;CONTE, 2016, p.28)

A passagem para o século XXI traria consigo o grande aprimoramento da rede mundial, paralelamente ao das tecnologias, com uma grande evolução e avanço em todos os aspectos possíveis e imagináveis, como velocidade e usabilidade, dentre outros. (FIORILLO;CONTE, 2016, p.29)

A Internet, também chamada como rede mundial, é uma rede que interliga computadores pessoais e dispositivos tecnológicos em escala mundial, unindo e compartilhando dados dando visibilidade a usuários domésticos, empresas, governos e qualquer dispositivo interligado. (IESDE, 2015, s.p.)

Neste mesmo sentido, Sadler (1996, p.9) ressalta que “a internet não é uma única rede de computadores, mas uma rede de redes. Ela, em outras palavras, é uma rede ampla que conecta várias redes menores umas com as outras”.

Geralmente os dados na internet ficam armazenados em servidores de dados que disponibilizam e organizam as informações por meio de sites ou endereços alternativos (IESDE, 2015, s.p.)

De acordo com Albertin (2001, p. 41)

> Atualmente, a internet (Intercontinentel Networks) é um sistema de distribuição da informação espalhado em vários países. Sua infra-estrutura muito geral atinge não apenas as aplicações de TI, tais como vídeo sob demanda ou home shopping, mas também uma grande lista de serviços baseados em computador, tais como e-mail, EDI, publicação de informação, recuperação de informação e videoconferência.

Paralelamente aos avanços da Internet, as tecnologias rapidamente também avançam para que possam acompanhar o ritmo e satisfazer aos usuários de forma que estejam adaptados as suas realidades, bem como aos seus cotidianos. (CRESPO, 2011, p.31)

Logo, surgem novas tecnologias que destacam a necessidade de acesso a Internet pela imensa diversidade de equipamentos de comunicação, como cita Albertin (2001, p. 41) “O ambiente da internet é uma combinação única de serviço postal, sistema de telefonia, pesquisa bibliográfica, supermercado e centro talk show que permite as pessoas compartilhar e comprar informações”.

Destarte, Albertin (2001, p. 42) enfatiza a troca rápida de informações com o uso da tecnologia e com um custo barato, como principais qualidades da internet.

Por fim, cabe concluir que atualmente a rede mundial de computadores, ou seja, a internet passou a fazer parte do cotidiano de toda a sociedade da informação possibilitando a interligação todos os computadores e dispositivos tecnológicos do mundo e estreitando a comunicação entre as pessoas, de forma a ditar novos costumes para a sociedade.

2.2.6 Navegadores de Acesso a Internet

Posta a definição e características da internet, passa-se a apresentar a forma mais comum e popular de acessar a internet, ou seja, o meio como é feito o acesso, sendo este através dos programas navegadores.

Os navegadores são programas, contidos no computador ou dispositivo tecnológico, que são utilizados para possibilitar ao usuário a acessar os dados dispostos na internet.

Estes navegadores também são conhecidos com outras nomenclaturas técnicas, entretanto a mais comum é browser, como expõe Bozza (2011, s.p.) “conhecidos como web browsers ou, simplesmente, browsers, os navegadores são uma espécie de ponte entre o usuário e o conteúdo virtual da Internet”.

Esta ferramenta é utilizada para a consulta, interpretação e exibição de dados, denominada também como o browser ou navegador, os quais tem-se como exemplos alguns dos mais comuns como o Internet Explorer, Chrome, Opera, Firefox e outros. (IESDE, 2015, s.p.)

Acerca dos navegadores, Vieira (2009, p.15) expõe que “com o advento dos novos navegadores que permitem a navegação com abas, é cada vez mais difícil manter o internauta em um único site por um longo período”.

Isto se dá em função de que dos atuais navegadores estão acompanhando a evolução dos dispositivos tecnológicos, bem como a vontade e a necessidade do usuário e da sociedade em acessar vários dados ao mesmo tempo.

Logo, os navegadores são de fundamental importância, pois são estes que fazem a interface entre a internet e os usuários, possibilitando a facilitação e a otimização no uso da rede mundial de computadores.

2.2.7 E-mail

A internet traz consigo a possibilidade de comunicação entre as pessoas, sendo um das formas mais comuns através da utilização de e-mails.

O termo e-mail (eletronic mail em inglês) é usado para o sistema de transmissão e recepção de mensagem de eletrônica. (PINTO, 2011, p.3)

O e-mail ou correio eletrônico, como também é conhecido, é uma forma de comunicação pela internet como se fora uma correspondência, onde um usuário a partir de um determinado endereço envia a mensagem para outro usuário que recebe por meio de um outro endereço, ou seja:

> O correio eletrônico é bastante parecido com a correspondência de papel; a única diferença é que ele faz a entrega muito mais rápida e barata. Cada mensagem do correio eletrônico da Internet contém um endereço informando para onde ela deve ir, um endereço de onde ela veio e um envelope com uma carta dentro. (SADLER, 1996, p.13)

Atualmente, não há dúvidas de que o e-mail tornou-se umas das formas mais populares utilizadas e importantes de comunicação pela internet.

2.2.8 Redes Sociais

A evolução da tecnologia, principalmente da internet e a globalização, implicam de forma significativa no avanço da sociedade.

Destarte, a comunicação vem tomando rumos cada vez mais facilitadores, onde basta a pessoa estar conectada a internet para poder se comunicar com qualquer outra pessoa, em qualquer outro local do mundo.

> Com o estreitamento da comunicação, por conta do avanço do tecnológico e da globalização, onde ambos ditam as tendências da sociedade moderna, esta vai aos poucos absorvendo e adaptando-se sempre ao contexto atual, e principalmente os frutos provindos da Internet. (TELLES, 2006, p.35)

Neste sentido, surgem diversas ferramentas de comunicação. Entretanto, as ferramentas que apresentam grande impacto na sociedade e em sua cultura são as redes sociais.

As redes sociais surgem com maior força no Brasil a partir do século XXI. (FIORILLO;CONTE, 2016, p.117)

Os sites de redes sociais tem o objetivo de servir como um local virtual para que as pessoas possam ter acesso, via internet, a pessoas de seu laço de

convívio social, preferência ou particularidade, bem como, traz ainda a possibilidade de criação de novos vínculos, ou ainda de se expressar perante a sua rede. (FIORILLO;CONTE, 2016, p.117)

Para Wendt e Jorge (2012, p.95) “quando falamos de mídias e/ou redes sociais estamos mencionando as diversas formas de relacionamento através de redes disponíveis na internet”.

Telles (2006, p.22) conceitua um dos sites de rede social como “grande banco de dados sobre quem é amigo de quem, ou seja, sobre rede de amizades”. Este mesmo autor conclui o seu raciocínio citando que o objetivo do site como rede social “é ajudar seus membros a criar novas amizades e manter relacionamentos”.

Dentre todas as redes sociais, as de uso mais comum, ou seja, as mais conhecidas e populares são ou foram: o Orkut, com o papel de precursor; as atuais redes sociais como Facebook, Twitter, Instagram ou ainda o Whatsapp que além de comunicador instantâneo, também funciona como rede social.

As redes sociais têm uma grande influência na cultura e na sociedade brasileira. Ano após ano cresce o número de usuários na internet e consequentemente o número de usuários cadastrados nos sites de redes sociais. (VIEIRA, 2009, p.14)

Para Vieira (2009, p.14), o crescimento de usuários na redes sociais está impactando diretamente no crescimento de usuários de Internet no Brasil, ou seja, “o fato é que a disseminação das redes de relacionamento/sociais foi uma forte alavanca para o crescimento de usuários de Internet no Brasil”.

Por fim, é importante ressaltar que o uso dos sites de redes sociais, assim como influencia no grande número de usuários na internet, impacta também diretamente na sociedade que passa a ter novos hábitos e renovações constantes, enfatizando a sociedade da informação.

3 CRIMES VIRTUAIS

O conceito de crimes virtuais pode ser visualizado neste capítulo, porém cumpre compreender anteriormente o conceito de crime ou delito, bem como tratar sobre a nomenclatura do referido tema.

3.1 CRIME/DELITO

O conceito de crime é analisado por doutrinadores sobre diversos aspectos.

No prisma de conceito material de crime, Ishida (2009, p.51) refere-se ao crime como "violação de um bem penalmente protegido. É um critério ou parâmetro sobre o que o direito penal deve punir", ou seja, quando um bem tutelado é atingido, caracteriza-se crime e cabe punição.

O conceito formal de crime é o prisma que, segundo Ishida (2009, p.51) "é a conduta proibida por lei decorrente da política criminal adotada. É a visão do legislador sobre quais bens jurídicos devem ser tutelados". Este conceito disciplina prevendo, por meio de leis, as condutas que podem ou não serem realizadas.

Por fim, no prisma do conceito analítico de crime, para alguns, também denominado conceito formal, Ishida (2009, p.51) enfatiza que "constitui a essência do estudo do crime no direito penal, sem dúvida, a parte mais importante tanto da parte geral como da parte especial".

Isto posto, cumpre salientar que o crime será abordado através do aspecto analítico ou formal para alguns autores, por ser o mais completo, tratando o mesmo em seu aspecto geral e em lato sensu.

Ainda que se pese a abordagem de forma geral, o conceito de crime por si somente é um tanto quanto complexo de ser apresentado, haja vista os diferentes posicionamentos por parte dos doutrinadores acerca do tema.

Para Capez (2005, p.107) "crime é todo fato típico e ilícito". O mesmo autor detalha ainda, discorrendo sobre a sua concepção bipartida sobre crime que

“em primeiro lugar deve ser obsevada a tipicidade da conduta. Em caso de positivo, e só neste caso, verifica-se se a mesma é ilícita ou não”.

Este conceito também é citado por Jesus (2008, p.152), onde o autor destaca que “são características do crime sob o aspecto formal: 1º) o fato típico; e 2º) a antijuricidade” onde o fato típico é definido como “comportamento (positivo ou negativo) que provoca resultado e é previsto na lei penal como infração” e a antijuricidade “é a relação de contrariedade entro o fato típico e o ordenamento jurídico”.

Por outro lado, outra corrente disciplina o tema de forma a divergir o entendimento anterior, uma vez que além do fato típico e da antijuricidade, ainda complementam o conceito de crime, a culpabilidade que inclusa caracteriza a teoria da tripartição.

Destarte, a culpabilidade é definido por Nucci (2011, p.300) como “importante elemento do crime, na medida em que representa o seu enfoque subjetivo, isto é, dolo e culpa”.

Acerca deste conceito, como discorre Bitencourt (2007, p.210) definindo que “o conceito analítico, predominante, passou a definir o crime como ação típica, antijurídica e culpável”.

Neste diapasão, Nucci (2011, p.173) conceitua o crime, discorrendo de forma minuciosa que:

> Trata-se de uma conduta típica, antijurídica e culpável, vale dizer, uma ação ou omissão ajustada ao modelo legal de conduta proibida (tipicidade), contrária ao direito (antijuricidade) e sujeita a um juízo de reprovação social incidente sobre o fato e seu autor, desde que existam imputabilidade, consciência potencial de ilicitude e exigibilidade e possibilidade de agir conforme o direito.

Logo, o que pode-se verificar é que este conceito , provindo da tripartição é mais amplo e abrangente do que o apresentado pela corrente que apoia a teoria da bipartição, anteriormente apresentada.

Há ainda quem aborde o crime por meio da denominação delito, como no caso de Crespo (2011, p.48) disciplinando sobre os crimes virtuais, tratando estes com a nomenclatura de “delitos informáticos”.

O delito na esfera penal é abordado como se fosse sinônimo do crime, umas vez que grande parte dos autores o trazem como o próprio crime, como observa-se por meio de uma das definições de Bitencourt (2007, p.205):

> A atual concepção quadripartida do delito, concebido como ação, típica, antijurídica e culpável (essa concepção pode ser definida como tripartida, considerando comento os predicados da ação, tipicidade, antijuricidade e culpabilidade), é o produto de construção recente, mais precisamente, do final do século XIX.

Neste sentido, também aborda de mesma forma, quando trata de uma das variações do conceito de crime, o qual cita como delito, no tocante aos seus critérios conforme salienta Jesus (2008, p.148) “O quarto critério visa ao aspecto formal e material do delito, incluindo na conceituação a personalidade do agente”.

Isto posto, cumpre salientar que independente da nomenclatura de crime ou delito, o conceito de crime, objeto ainda de divergência na doutrina contemporânea, tem fundamental importância para que se possa compreender o tema do presente trabalho.

Destarte, vistas as diversas definições de crimes, passa-se a abordar os crimes virtuais.

3.2 CRIMES VIRTUAIS

Adentrando ao tema crimes virtuais, é importante que se tenha anteriormente, a compreensão da nomenclatura e do conceito.

3.2.1 Nomenclatura

Inicialmente, antes de conceituar os crimes virtuais, é importante pontuar uma parte do referido tema e que é relativamente básico perante aos leigos, mas que causa polêmica e divergência entre os doutrinadores que abordam o

assunto. Trata-se da nomenclatura as diversas condutas ilícitas realizadas por meio de algum tipo de dispositivo tecnológico. (CRESPO, 2011, p.47)

Neste sentido, Crespo (2011, p.47) utiliza a denominação “Crimes Digitais” e cita algumas das diversas denominações dadas:

> Verificam-se pois, várias denominações, dentre as quais “crimes de computador”, “infrações por meio de computador”, “crimes por meio de informática”, “fraude informática”, “delinquência informática”, “crimes digitais”, “computer-related crimes”, “cybercrimes” ou “crimes cibernéticos”.

Para Wendt e Jorge (2012, p.1) utiliza-se como nomenclatura o termo “crimes cibernéticos” como sinônimo de crimes de virtuais por entender que se trata de um termo genérico, porém se tratando das especificidades também pode-se abordar com outras denominações como crimes cometidos por meios eletrônicos, crimes de alta tecnologia, cibercrimes, crimes digitais, crimes de informática dentre outros termos mais.

Segundo Fiorillo e Conte (2015, p.185), a utilização da denominação “crimes informáticos”, “permite abarcar um campo maior levando em consideração toda a delinquência relacionada com a informática e as novas tecnologias”.

Em uma linha parecida de raciocínio, Zanellato (2002, p.180) denomina como “ilícitos informáticos”.

A nomenclatura “delitos informáticos”, é umas das primeiras a serem utilizada pela doutrina para os crimes praticados virtualmente. (CRESPO, 2011, p. 48)

Isto posto e enfatizando que, em que se pese o não consenso dentre os doutrinadores que abordam o tema e a diversidade de nomenclaturas acerca do tema, todas abarcando as diversas condutas ilícitas realizadas por algum tipo de dispositivo tecnológico, a que será utilizada neste trabalho é a de “Crimes Virtuais” por entender-se que a realização das condutas são dadas em um ambiente virtual e por assim ser tratada por vários autores como Paiva (2012, p.9), Carneiro (2012, s.p.), Oliveira e Dani (2011, s.p.), Ribeiro (2013, p.19) e Medeiros (s.d;s.p.).

3.2.2 Conceito

A evolução tecnológica e a popularização da internet têm gerado grandes impactos na sociedade. Não diferente, as ciências jurídicas também passaram a ser impactadas, principalmente na seara criminal, uma vez que o crescimento do uso da tecnologia e da internet possibilita a prática de crimes complexos. (SANTOS, 2009, p.29)

Estes crimes são aqui abordados como crimes virtuais.

Jesus e Milagre (2016, s.p.) conceituam crimes virtuais como:

> [...] como 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 das atividades informática. Assim, é um ato típico e antijurídico, cometido através da informática em geral, ou contra um sistema, dispositivo informático ou redes de computadores.

Os crimes virtuais são os delitos praticados contra ou por intermédio de computadores, ou seja, são condutas indevidas praticadas por um computador. (WENDT;JORGE, 2012, p.18)

Neste sentido, os crimes virtuais ainda podem abranger diversas condutas e são aqueles ilícitos praticados não somente por computador ou informática, mas sim praticados por meio da telemática, sendo esta uma expressão utilizada para serviços de informática por meio de telecomunicações. (CRESPO, 2011, p.51)

Em uma abordagem mais ampla, pode-se conceituar os crimes virtuais como ilícitos cometidos por intermédio de Internet ou com o auxílio desta, de forma que cause algum tipo de dano a vítima, ou ainda, práticas ilícitas penais contra computador ou contra as informações contidas no mesmo. (FIORILLO;CONTE, 2016, p.187)

Por fim, os crimes virtuais também podem ser conceituados como sendo às condutas de acesso não autorizado a sistemas informáticos, ações destrutivas nesses sistemas, a interceptação de comunicações, modificações de dados, infrações a direitos de autor, incitação ao ódio e descriminação, escárnio religioso, difusão de pornografia infantil, terrorismo, entre outros. (PINHEIRO, 2013, s.p.)

Diante da exposição dos conceitos referentes a crimes virtuais, fica claro que crimes virtuais são crimes cometidos por meio de dispositivo tecnológico, sendo este cometido única e exclusivamente por meio de tecnologia ou usando a tecnologia apenas como meio, onde a conduta, outrora, poderia ser cometida sem o uso da mesma.

4 CLASSIFICAÇÃO E TIPIFICAÇÃO DOS CRIMES VIRTUAIS

A classificação atual dos crimes virtuais, de acordo com a doutrina, basicamente refere-se a divisão deste tipo de crime em: crimes já previstos pelo ordenamento jurídico penal e realizados por meio de dispositivo tecnológico; e pelos crimes também realizados por meio de computadores, mas que somente podem ser realizados desta forma e atingem bens jurídicos específicos relacionados a tecnologia, assim como discorre e classifica Crespo (2011, p.63) acerca do tema:

> Neste sentido, podemos dizer que todas as condutas praticadas contra bens jurídicos informáticos (sistemas, dados) são delitos de risco informático ou próprios, ao passo que aquelas outras condutas que se dirigem contra bens jurídicos tradicionais (não relativos à tecnologia) são crimes digitais impróprios.

Parte da doutrina que aborda o tema acredita que esta forma, por ser mais didática, dentre as muitas classificações doutrinárias usadas para definir e classificar crimes virtuais, seja a mais próxima da realidade dos fatos, ou seja, a divisão entre crimes virtuais próprios e crimes virtuais impróprios. (CARNEIRO, 2012, s.p.)

Outros doutrinadores tratam a divisão de crimes virtuais com outras denominações, porém dentro de uma mesma linha de raciocínio, como no caso de Wendt e Jorge (2012, p.19) que prevê a divisão da seguinte forma: “os crimes cibernéticos se dividem em “crimes cibernéticos abertos” e “crimes exclusivamente cibernéticos”“.

Nesta mesma linha, estes crimes também são denominados como crimes informáticos puros ou impuros. (BRITO, 2014, s.p.)

Logo, o que há em comum em todas as classificações apresentadas a atribuição aos dispositivos tecnológicos, dados e informações como bens jurídicos tutelados e os mesmos como meio/instrumento para a prática da conduta com o objetivo de lesionar outros bens, apenas diferenciando o fato de somente poderem ser realizados por este meio/instrumento. (CRESPO, 2011, p.63)

4.1 CRIMES VIRTUAIS PRÓPRIOS

Os crimes virtuais próprios são crimes que somente podem ser praticados pela internet, ou seja, condutas que somente podem ser realizadas através da rede mundial de computadores. (BRITO, 2014, s.p.)

Neste sentido, Jesus e Milagre (2016, s.p.) definem crimes virtuais próprios como aqueles “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”.

Wendt e Jorge (2012, p19) complementam o conceito de crimes próprios virtuais discorrendo que “eles somente podem ser praticados com a utilização de computadores ou de outros recursos tecnológicos que permitem o acesso à internet”.

Além disso, ressalta-se que nesta modalidade de crime virtual onde o sujeito utiliza necessariamente o sistema informático do computador do sujeito passivo, onde o computador como sistema tecnológico é usado como objeto e meio para a execução do crime. (CARNEIRO, 2012, s.p.)

Os crimes virtuais próprios também podem ser definidos como conduta praticada contra bens jurídicos informáticos. (CRESPO, 2011, p.63)

No tocante ao bem jurídico atingido neste tipo de crime, Crespo (2011, p.63) é perfunctório ao discorrer sobre crimes virtuais próprios como “delitos cujos bens jurídicos atingidos são primordialmente os sistemas informatizados ou telecomunicações ou dados”.

Entretanto, o bem jurídico tutelado nos crimes virtuais próprios, no entendimento de Silveira (2015, s.p.), o qual destaca o artigo 154-A, o qual é abordado no tópico seguinte, “chega-se ao bem jurídico tutelado como sendo a liberdade individual, a privacidade e a intimidade das pessoas como um todo”.

Neste diapasão, pode-se complementar que são crimes que violam inicialmente a informação ou a privacidade como bem jurídico principal, e que de forma secundária atingem os dados ou sistemas. (CRESPO, 2011, p.57)

A seguir expõem-se as condutas desta modalidade que podem ser caracterizadas como crime, bem como o enquadramento na tipificação penal de cada uma.

4.1.1 Acesso Não autorizado (Invasão)

O acesso não autorizado, também conhecido como invasão ou ainda como hacking, é a conduta de acessar indevidamente um sistema informático, seja para obter prestígio perante aos seus pares ou ainda para que se obtenha algum tipo de vantagem ou manipulação de dados. (CRESPO, 2011, p.64)

A tipificação desta conduta é prevista atualmente no Código Penal Brasileiro, o qual teve redação alterada pela Lei nº 12.737 de 30 de novembro de 2012, lei esta que foi denominada popularmente como "Lei Carolina Dieckmann". (MINISTÉRIO PÚBLICO FEDERAL - PROCURADORIA DA REPUBLICA NO ESTADO DE SÃO PAULO - GRUPO DE COMBATE AOS CRIMES CIBERNÉTICOS, s.d; s.p.)

Tal nomenclatura não foi dada apenas por conta do caso ocorrido com a referida atriz de uma emissora de tv, onde a mesma teve fotos furtadas em meio a manutenção de seu computador pessoal. Não bastasse o furto, a atriz ainda foi chantageada pelos detentores das fotos para que houvesse compensação financeira para que não fossem divulgadas pela internet. (BERTOLDI, 2013, s.p.)

Ocorre que neste mesmo tempo, por coincidência, havia um projeto em tramitação abarcando o tema, logo acabou-se dando nome à lei por conta do caso estar em voga. (BERTOLDI, 2013, s.p.)

Esta lei tem em seu conteúdo principal a invasão de dispositivo informático, bem como suas consequências. Em uma das alterações realizadas pela lei é incluído o artigo 154-A ao Código Penal, onde o mesmo faz menção a crimes cibernéticos propriamente ditos disciplinando que:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar

> vulnerabilidades para obter vantagem ilícita.Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.) (BRASIL, 1940, s.p.)

Logo, é um artigo que prevê a conduta de invasão de dispositivo informático de outrem, sem autorização, violando mecanismo de segurança, independente de estar conectado ou não a alguma rede com o intuito de obter, alterar ou destruir dados ou informações.

Há ainda alguns específicos previstos para a invasão.

Neste sentido, ressalta-se o crime contra um rol de agentes específicos de acordo com o parágrafo 5º do mesmo artigo 154-A do Código Penal Brasileiro, prevendo aumento de um terço á metade nos crimes praticados contra:

> [...]I - Presidente da República, governadores e prefeitos; II - Presidente do Supremo Tribunal Federal; III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (BRASIL, 1940, s.p.)

Esta mesma conduta é tipificada também com especificidade ao âmbito político, no tocante ao acesso de sistemas de apuração de votos, através da Lei 9.504/97 a qual dispõe que:

> Art. 72 – Constituem crimes, puníveis com reclusão, de cinco a dez anos: I - Obter acesso a sistema de tratamento automático de dados usado pelo serviço eleitoral, a fim de alterar a apuração ou contagem de votos; (BRASIL, 1997, s.p.)

Há ainda, por fim, previsão no ordenamento jurídico brasileiro relacionada à invasão de dispositivos nos artigos 313-A e 313-B do Código Penal, os quais se referem a conduta realizada por funcionário público contra a Administração Pública, porém para Crespo (2011, p.69) “nem sempre o acesso é desautorizado”.

Destarte, o artigo 313-A disciplina que:

> Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: Pena – reclusão, de 2 (dois) a 12 (doze) anos, e multa.; (BRASIL, 1940, s.p.)

Neste sentido, o artigo 313-A refere-se ao funcionário público que visa obter vantagem indevida para si ou para outrem, ou para causar dano, de forma que facilite ou que insira dados falsos, ou que exclua sem justificativa, dados corretos existentes nos sistemas informatizados ou em banco de dados da Administração Pública, prevendo punição de 2 a 12 anos de reclusão e multa.

Já o artigo 313-B do Código Penal Brasileiro disciplina que:

> Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente: Pena – detenção, de 3 (três) meses a 2 (dois) anos, e multa.Parágrafo único. As penas são aumentadas de um terço até a metade se da modificação ou alteração resulta dano para a Administração Pública ou para o administrado. (BRASIL, 1940, s.p.)

Logo, o funcionário público que modificar ou alterar os sistemas informatizados sem justificativa, diga-se, autorização ou solicitação de autoridade competente, deverá ser punido com a detenção de três meses a dois anos. Este tipo de crime prevê ainda, por meio de seu parágrafo único, o aumento da pena de um terço a metade da pena em caso do resultado gerar dano a Administração Pública.

No tocante a invasão de dispositivo realizada por funcionário público, o Tribunal de Justiça do Rio Grande do Sul apresenta uma decisão acerca do tema.

> CRIME CIBERNÉTICO - FUNCIONÁRIO PÚBLICO - DELITO SEM COMPLEXIDADE - ESSÊNCIA DOS CRIMES DE ALTERAÇÃO DE SISTEMA INFORMATIZADO - CIRCUNSTÂNCIAS JUDICIAIS FAVORÁVEIS - PENA BASE FIXADA NO MÍNIMO. Funcionário da CEEE que transfere no sistema, débito de fornecimento de energia para pessoa fictícia. Crime cibernético tipificado no art. 313-A do Código Penal. Sendo favoráveis todas as circunstâncias judiciais, a pena base deve situar-se no mínimo. Não se pode entender como complexa, conduta de agente nessas condições, já que a alteração de dados em sistema informatizado é da própria...(TJ-RS - ACR: 70043570068 RS, Relator: Gaspar Marques Batista, Data de Julgamento: 06/10/2011, Quarta Câmara Criminal, Data de Publicação: Diário da Justiça do dia 13/10/2011)

A decisão é referente a fixação da pena base de um funcionário público que alterou dados no sistema informatizado que controla o fornecimento de energia, e que foi enquadrado no artigo 313-A do Código Penal.

Por fim, cabe ressaltar que o acesso não autorizado ou invasão é a conduta mais comum dos crimes virtuais, principalmente porque a partir dela são desencadeadas outras condutas.

4.1.2 Obtenção dados e transferência ilegal de dados

A obtenção de dados e a transferência ilegal de dados, são condutas que podem ser dadas em diversas formas, entretanto algumas são mais comuns no cotidiano da sociedade atual. A principal delas é por meio de spywares ou espiões que são programas que rastreiam informações contidas no dispositivo tecnológico. (CRESPO, 2011, p.70)

Sobre os spywares ou espiões, estes programas foram criados com o objetivo de serem utilizados por empresas para que estas pudessem identificar os hábitos de possíveis clientes em potencial e consequentemente usar as informações capturadas afim de direcionar estratégias de publicidade e propaganda, porém, com o passar do tempo, estes programas passaram a ser utilizados ilicitamente. (BITTENCOURT, 2013, s.p.)

Os spywares ou espiões podem ser encontrados em alguns formatos, dentre os quais é possível citar: os cookies, uma espécie de spyware positivo, uma vez que são programas que são utilizados para envio de informações coletadas pela internet para as empresas, auxiliando-as principalmente em estratégias de propaganda; os trojans ou cavalo de tróia que são programas que aparentam utilidade mas que escondem em si atividade maliciosa como coleta e envio de dados privados; e os keyloggers que são programas que tem por objetivo captar todos os comandos inseridos nos dispositivos, seja por meio de teclado convencional, teclado virtual ou ainda cliques, destacando principalmente a captura de senhas, números de cartão de crédito, e demais informações. (CRESPO, 2011, p.70)

A previsão da conduta de obtenção de dados é disciplinada pelo parágrafo 3º do art. 154-A do Código Penal Brasileiro:

> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave. (BRASIL, 1940, s.p.)

A partir da obtenção de dados é possível a ocorrência de transferências dos mesmos para si ou ainda para outrem, ou seja, consiste em deslocar os dados para algum outro dispositivo tecnológico.

A previsão para a conduta de transferência de dados é prevista pelo parágrafo 4º do artigo 154-A do Código Penal Brasileiro, o qual disciplina que "na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos. (BRASIL, 1940, s.p.)

4.1.3 Dano Informático

O dano informático tem atualmente uma abordagem prevista basicamente por dois prismas, sendo estes: o dano ao bem material, ou seja, dano causado a coisas materiais como o computador, o monitor, a impressora, pendrives, discos rígidos ou ainda dispositivos tecnológicos em geral dotados de algum valor econômico; e o dano ao bem imaterial, ou seja, dano causado a coisas imateriais abarcando principalmente os dados os quais são intangíveis e de complicada valoração econômica. (CRESPO, 2011, p.71-73)

Destarte, no que toca a previsão de dano informático as coisas materiais, o Código Penal Brasileiro dispõe por meio do art. 163 que: "Art. 163 - Destruir, inutilizar ou deteriorar coisa alheia: Pena - detenção, de um a seis meses, ou multa". (BRASIL, 1940, s.p.)

No caso de dano informático a coisas imateriais, ou seja, adulteração ou destruição de dados, o Código Penal Brasileiro, mais especificamente através do art. 154-A, disciplina que :

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.) (BRASIL, 1940, s.p.)

Este artigo é claro com relação à tipicidade no caso de dano informático no sentido de geração de danos a dados ou informações, prevendo

neste caso a detenção de 3 meses a 1 ano para quem cometa esta conduta ilícita de forma a atingir o bem.

Logo, conclui-se que em ambos os casos de danos, material ou imaterial, há a tipicidade prevista para esta conduta no Código Penal Brasileiro.

4.1.4 Vírus e sua Disseminação

Define-se vírus por programa que se anexa a outros programas ou sistemas e executa comandos pré-definidos, podendo gerar ao usuário lentidão, incapacidade de acesso a dados ou ainda a perda a total dos dados. (CRESPO, 2011, p.74)

Logo, destaca-se o objetivo principal de atravancar, destruir ou ainda dificultar o funcionamento de outros programas, bem como de dispositivos tecnológicos. (CRESPO, 2011, p.74)

O vírus é uma espécie de malware. Os malwares, termo criado para denominar softwares maliciosos, são programas que tem por finalidade gerar algum tipo de ilícito danoso. (BITTENCOURT, 2013, s.p.)

A previsão das condutas de produção e de difusão de vírus tem pena de detenção de três meses a um ano e multa, sendo estas abordadas através do art. 154-A do Código Penal Brasileiro, em seu parágrafo primeiro discorrendo que “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”. (BRASIL, 1940, s.p.)

4.1.5 Divulgação ou utilização indevida de informações

A conduta de divulgação ou utilização indevida de informações, ainda que realizada pela internet, é atualmente prevista por meio do caput do art. 154 do Código Penal Brasileiro:

> Art. 154 - Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem: Pena - detenção, de três meses a um ano, ou multa. (BRASIL, 1940, s.p.)

Tal conduta também é prevista também através da combinação do artigo 154-A por meio do parágrafo 4º.

O parágrafo 4º do artigo 154-A aumenta a pena de um a dois terços do previsto no parágrafo 3º do mesmo artigo, que disciplina sobre a obtenção dos dados, se houver a divulgação, comercialização ou a transmissão a terceiro dos dados ou informações obtidas, ou seja, disciplina-se que "na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos". (BRASIL, 1940, s.p.)

Chama-se atenção para uma das formas de realização da divulgação ou utilização de informações, que são os casos em que usuários fazem seus cadastros em sites, seja para compras ou qualquer ação interativa junto à internet, em que insira os seus dados pessoais e que estes sejam manipulados ou abusados, oriundos de acesso não autorizado ou não. (CRESPO, 2011, p.80)

Cabe ressaltar inclusive que tal conduta atinge também o direito a privacidade, o qual é disciplina pelo inciso X do artigo 5º da Constituição Federal, da seguinte forma: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação". (BRASIL, 1988, s.p.)

Destarte, enfatiza-se que as pessoas cada vez mais realizam as mais diversas interações pela internet, sejam acessos e postagens as redes sociais, compras ou ainda outras operações pessoais ou financeiras, e que o que ocorre é que as informações inseridas neste contexto pelo usuário, podem ou não trazer penalidades as pessoas que façam o uso sem autorização, uma vez que constitui um limite natural ao direito à informação. (PINHEIRO, 2013, s.p.)

Nesta conduta de divulgação ou utilização indevida de informações, também cabe uma das principais e mais comuns das formas de realizá-la pela internet ou dispositivo tecnológico é por meio do spam, que nada mais é do que o recebimento de e-mails ou mensagens indesejadas ou não solicitadas, que outrora foram enviadas por um spammer, ou seja, pessoas especialistas em disparar e-

mails, para vários endereços ao mesmo tempo, e sendo isto realizado por meio de algum dispositivo tecnológico conectado a internet. (MILAGRE, 2013, s.p.)

O caso do spam especificamente há quem sustente que quem realiza o envio de spam incorre na prática ao ilícito do crime de dano, discorrido através do art. 163 do Código Penal Brasileiro, entretanto isto somente há a possibilidade de ocorrer em casos excepcionais como o envio de um grande número de mensagens ao mesmo tempo de forma a gerar lentidão no acesso à rede ou internet ou então que devido ao grande número de mensagens recebidas decorresse algum dano aos dispositivos tecnológicos. (CRESPO, 2011, p.79)

Um pouco mais além, vislumbra ainda sobre o spam e o envio de mensagens ou e-mails indevidos que, onde esta prática corriqueira deve ser observada pela ótica de geração danos, sejam estes: danos morais, uma vez que atenta contra a dignidade pela imposição e invade a privacidade da vítima que encontra-se em estado vulnerável perante a este tipo de conduta, e danos materiais pela poluição do meio-ambiente por conta do tempo de uso de energia elétrica para que os usuários apagam os spams recebido. (CARNEIRO, 2012, s.p.)

Salienta-se também que considere-se a obtenção e utilização de dados e informações na esfera de espionagem industrial, conduta que será exposta adiante neste trabalho. (CRESPO, 2011, p.80)

4.1.6 Embaraçamento ao funcionamento de sistemas

O embaraçamento ao funcionamento de sistemas geralmente se dá por ataques chamados de DoS (Denial of Service), na tradução “negação de serviço”, onde. (CRESPO, 2011, p.80)

Segundo Crespo (2011, p.80) na conduta de embaraçamento ao funcionamento de sistemas “computadores são utilizados para tirar de operação um serviço ou outros computadores conectados a internet”, como por exemplo em na geração de sobrecarga de processamento de dados de um computador, onde devido a geração de grande tráfego de dados na rede, o serviço ou o computador fique indisponível.

Há ainda uma variação do DoS, onde a denegação de serviço é realizada de forma distribuída, ou seja, ataques em que vários computadores, por comando de um computador específico, enviam pacotes ou solicitações para um determinado computador ou serviço com o objetivo de torná-lo indisponível. Este tipo de ataque é chamado de DDoS (Distributed Denial of Service), na tradução "negação de serviço distribuído". (WENDT;JORGE, 2012, p.25)

Esta conduta está tipificada pelo Código Penal Brasileiro, em seu artigo 266, oriunda da "Lei Carolina Dieckmann" passando a disciplinar sobre a "Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública", discorrendo que "interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento: Pena - detenção, de um a três anos, e multa". (BRASIL, 1940, s.p.)

O parágrafo 1º do artigo 266 do Código Penal faz referência a conduta prevista neste artigo, porém quando o atingido é de utilidade pública, ou seja, prevê que quem "incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento" (BRASIL, 1940, s.p.)

Acerca do parágrafo 1º do artigo 266, acima referido, Crespo (2011, p.81) alerta para os casos em que um ataque possa vir a retirar um site de alguma grande loja na internet, redes de grandes escritórios ou grandes empresas, ou ainda para empresas provedoras de internet ou bancos, em que todas estas podem vir a ter um prejuízo imensurável, além de prejudicar outros usuários.

Já o parágrafo 2º do artigo 266 do Código Penal, prevê o dobro da pena e o crime é cometido quando a ocasião dor em estado de calamidade pública. (BRASIL, 1940, s.p.)

4.1.7 Engenharia Social e Phishing

A engenharia social é a utilização do artifício intelectual e de um conjunto de técnicas empregadas em um método que mascara a realidade, para fazer com que o a vítima acredite nas informações e envie dados pessoais aos

criminosos para que estes possam, a partir destes dados, executar as ações desejadas. (WENDT;JORGE, 2012, p.20)

A engenharia social é uma técnica de persuasão, praticada de má-fé, por uma pessoa, diga-se golpista, visando abusar da ingenuidade e da confiança de outra pessoa a fim de aplicar golpes, ludibriar ou obter dados pessoais importantes. (CENTRO DE ESTUDOS, RESPOSTAS E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL, 2012, p.115)

Os engenheiros sociais, como são chamadas pessoas que incorrem nesta conduta, usam técnicas a partir da emoção de seus alvos, usando dentre outras formas emotivas, o medo, a ganância, a simpatia e a curiosidade. Criada a motivação, o usuário presta assim as informações necessárias. (WENDT;JORGE, 2012, p.23)

No tocante a tipicidade desta conduta, orienta-se que a engenharia social só, pode levar a configuração de uma fraude ou estelionato, conforme disciplinado pelo art. 171 e seguintes, entretanto somada a invasão de dispositivo tecnológico, prevista no art. 154-A do Código Penal Brasileiro, pode configurar diversos crimes como dano, violação de direitos autorais, bem como a própria invasão do dispositivo. (CRESPO, 2011, p.82)

Já o phishing, na tradução especifica para este caso significa pescar, pode ser considerado uma modalidade da engenharia social, uma vez que parte do mesmo princípio de realização da fraude virtual, ludibriando a vítima para obtenção de dados pessoais importantes, ou seja, a “pesca dos dados”, entretanto a sua particularidade é o meio por onde se age é especificamente através do envio de mensagens eletrônicas. (CRESPO, 2011, p.83)

A intenção desta conduta é, assim como na engenharia social, chamar a atenção do de sua vítima em potencial, neste caso o usuário da mensagem eletrônica, apresentando temas diversos como nos casos de campanhas publicitárias, serviços, imagens impactantes de pessoas ou assuntos em destaque no momento. (CENTRO DE ESTUDOS, RESPOSTAS E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL, 2012, p.9)

Para Wendt e Jorge (2012, p.39) phishing é:

> [...] a conduta das pessoas que encaminham mensagens com a finalidade de induzir a vítima a preencher formulários com seus dados privados ou

> instalar códigos maliciosos, capazes de transmitir para o criminoso cibernético as informações desejadas

Os casos mais comuns que ocorrem tanto de engenharia social quanto de phishing, ou seja, por meio de sites falsos; e-mails que contenham links para acesso a sites falsos; e-mails que encaminham o usuário para o acesso a um site falso contendo programas que são instalados automaticamente no dispositivo do usuário, são os casos de captura de informações bancárias, de cartões de crédito, senhas em geral; e por fim, atualmente casos em mensagens postadas em redes sociais com falsos links. (CRESPO, 2011, p.82)

A tipicidade conduta phishing assim como a engenharia social, segundo Crespo (2011, p.85) é estelionato pelo fato de que o autor visa vantagem econômica, conforme disciplinado pelo artigo 171, discriminando que:

> 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. (BRASIL, 1940, s.p.)

O artigo 171 do Código Penal Brasileiro faz menção ao crime estelionato, prevendo que a pessoa que obtenha para si ou outrem vantagem de forma ilícita mediante a algum tipo de fraude será punido com a reclusão de um a cinco ano e mais multa prevista conforme lei.

Entretanto no caso do envio de e-mail encaminhando a instalação de programas maléficos que facilitam a invasão ao dispositivo e permitem o acesso indevido e a captura de dados ou informações para cometimento de fraude, o enquadramento cabe também ao art. 154-A do Código Penal Brasileiro:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita. Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa.) (BRASIL, 1940, s.p.)

Logo, este tipo de conduta por meio de dispositivo tecnológico pode ser tipificada pela combinação dos artigos 171 que é a previsão do crime normalmente utilizada, com o artigo 154-A que prevê a invasão ao dispositivo, neste caso para a obtenção dos dados e informações a serem usadas para o estelionato.

4.1.8 Intercepção Ilegal de Dados

A Constituição Federal de 1988 consagra a inviolabilidade das comunicações em geral como Direito Fundamental, conforme o seu art. 5º, em seus incisos X e XII disciplinando que:

> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal (BRASIL, 1988, s.p.)

Entretanto, não se trata de inviolabilidade absoluta, pois caso tenha-se autorização sob ordem judicial, para fins de investigação policial, a interceptação das comunicações telefônicas pode assim ser realizada. (CRESPO, 2011, p.86)

Em um primeiro momento de criação da Constituição Federal, em 1988, o texto lei tinha o objetivo de abarcar apenas interceptações de comunicações telefônicas. Com a evolução tecnológica e principalmente com a popularização da internet, atualmente possibilitando diversas formas de comunicação, foi necessário desenvolvimento de texto específico acerca do tema através da Lei 9296/1996, lei esta que aborda especificamente interceptações telefônicas. (CAVALCANTE, 2014, s.p.)

Neste mesmo sentido Wendt e Jorge (2012, p.125) enfatiza que “na interceptação das comunicações telemáticas aplica-se o disposto no artigo 5º, incisos X e XII da Constituição Federal, bem como a lei 9296/96”:

O parágrafo único, do art. 1º da lei 9296/96, lei que regulamenta o inciso XII, parte final, do artigo 5º da Constituição Federal de 1988, estende a aplicabilidade da lei de interceptação aos sistemas de informática, bem como a telemática.

O referido artigo discorre que:

> Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça. Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática. (BRASIL, 1996, s.p.)

Esta mesma lei 9296/1996, por meio de seu art. 10º criminaliza a interceptação de dados sem que haja autorização disposta em lei, conforme exposto:

> Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei. Pena: reclusão, de dois a quatro anos, e multa. (BRASIL, 1996, s.p.)

Cumpre salientar que não há como negar que a tanto a informática quanto a telemática são atualmente meios de comunicação, logo aplicam-se todos os dispositivos discorridos. (CRESPO, 2011, p.87)

Por fim, cabe concluir que aplicam-se para os casos dos crimes virtuais, no que toca a violação ilegal de dados, os mesmos dispositivos legais que são utilizados para os demais casos.

4.2 CRIMES VIRTUAIS IMPRÓPRIOS

Os crimes virtuais impróprios são condutas já conhecidas, crimes já de conhecimento da sociedade, uma vez que já são tipificados pelo ordenamento jurídico penal e que podem ser praticados por qualquer meio, inclusive pela internet. (Brito, 2014, s.p.)

Para Jesus e Milagre (2016, s.p.) crimes virtuais impróprios são aqueles 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;

Destarte, Wendt e Jorge (2012, p.19) cita esta modalidade de crime, onde o computador é tão somente o meio para a prática do crime, ou seja, “o computador é apenas o meio para a prática do crime, que também poderia ser cometido sem o uso dele”.

Em uma abordagem um pouco mais analítica, os crimes virtuais impróprios podem ser conceituados também da seguinte forma:

> Os crimes virtuais denominados impróprios são aqueles realizados com a utilização do computador, ou seja, por meio da máquina que é utilizada como instrumento para realização de condutas ilícitas que atinge todo o bem jurídico já tutelado, crimes, portanto que já tipificados que são realizados agora com a utilização do computador e da rede utilizando o sistema de informática seus componentes como mais um meio para realização do crime, e se difere quanto a não essencialidade do computador para concretização do ato ilícito que pode se dar de outras formas e não necessariamente pela informática para chegar ao fim desejado. (CARNEIRO, 2012, s.p.)

Estes tipos de crimes já estão tipificados em nosso ordenamento jurídico, porém com a utilização da internet dá-se uma nova roupagem justamente pelo fato de serem praticados por intermédio de dispositivos tecnológicos. (GATTO, 2011, s.p.)

Logo, este tipo de crime além de ser o já tradicionalmente tipificado no ordenamento agregando o uso de modernas tecnologias, representa que os ilícitos penais tradicionais, outrora tipificados, podem ser cometidos de uma nova forma, ou seja, por meio de novo modi operandi. (CRESPO, 2011, p.87)

A seguir, serão abordados de forma perfunctória, os principais tipos de crimes virtuais impróprios, para que se tenha uma visão breve e ampla da tipificação dos crimes desta modalidade de crime.

4.2.1 Ameaça

A ameaça, mesmo quando realizada mediante a algum tipo de dispositivo tecnológico, é um crime contra a liberdade individual, equiparando-se a ameaça prevista por meio do art. 147 do Código Penal Brasileiro, que disciplina que “Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave: Pena - detenção, de um a seis meses, ou multa”. (BRASIL, 1940, s.p.)

Para Nucci (2011, p. 705) “ameaçar significa procurar intimidar alguém, anunciando-lhe a ocorrência de mal futuro, ainda que próximo”.

Destarte, ameaçar alguém é tipificado como crime, uma vez que a conduta de intimidar alguém com objetivo de amedrontar e mediante a promessa de causar a vítima um mal injusto e grave, podendo ser o tipo de ameaça direta ou indireta, implícita ou explícita. (CRESPO, 2011, p.88)

Ressalta-se, que no tocante ao bem jurídico tutelado neste tipo de crime, se tratando da proteção à liberdade psíquica, ou seja, a tranquilidade de espírito da vítima. (ISHIDA, 2009, p.268)

Este tipo de crime é muito comum e normalmente a vítima procura a delegacia de polícia para comunicar o recebimento da ameaça por e-mail, redes sociais, mensagens de comunicadores instantâneos ou telefonemas. (WENDT;JORGE, 2012, p.105)

4.2.2 Participação em suicídio

O conceito de suicídio é apresentado por Ishida (2009, p.226) da seguinte forma: “O suicídio é a deliberada autodrestuição da vida (a própria pessoa deseja se matar)”.

No Brasil, o suicídio não é considerado crime, entretanto quem ajuda, instiga ou induz a outra pessoa a se matar responde por crime. (CRESPO, 2011, p.88)

Este tipo de crime é abordado pelo Código Penal Brasileiro, através do art. 122 que doutrina:

> Art. 122 - Induzir ou instigar alguém a suicidar-se ou prestar-lhe auxílio para que o faça: Pena - reclusão, de dois a seis anos, se o suicídio se consuma; ou reclusão, de um a três anos, se da tentativa de suicídio resulta lesão corporal de natureza grave. (BRASIL, 1940, s.p.)

Neste sentido, o artigo 122 prevê que a pessoa que por indução ou instigação auxiliar outrem ao suicídio será penalizado criminalmente com reclusão de dois a seis anos se o suicídio consumar ou em caso de tentativa a pena é de um a três anos.

Este tipo de crime também pode ser cometido pela internet, porém é necessário que se tenha eficácia e que seja contra pessoa determinada. (CRESPO, 2011, p.88)

Neste tipo de crime, o bem jurídico tutelado é a vida humana, sendo este um bem indisponível, uma vez que o ordenamento jurídico brasileiro não tem previsão alguma para o direito de morrer. (ISHIDA, 2009, p.226)

È importante se ter cuidado com condutas ofensivas, muito comuns, pela internet e principalmente em redes sociais, como o cyberbullying ou ainda páginas específicas que façam alusão ao suicídio de determinada pessoa, uma vez que estas condutas podem soar como induzimento ou instigação para o suicídio. (CRESPO, 2011, p.88)

4.2.3 Incitação e Apologia ao Crime ou a Criminoso

A incitação e a apologia ao crime ou a criminoso são condutas tipificadas no Código Penal Brasileiro, através dos arts. 286 e 287, os quais disciplinam sobre a punição de preparatórios de crimes.

O artigo 286 do Código Penal Brasileiro disciplina que “incitar, publicamente, a prática de crime: Pena - detenção, de três a seis meses, ou multa”. (BRASIL, 1940, s.p.)

A incitação ao crime é impelir, estimular ou instigar, publicamente a prática de crime, devendo a instigação realizada sobre pessoas determinadas ou indeterminadas da coletividade a praticar crimes específicos. (NUCCI, 2011, p.959)

Quanto à conduta ilícita de apologia ao crime, o artigo 287 do Código Penal Brasileiro disciplina que “fazer, publicamente, apologia de fato criminoso ou de autor de crime: Pena - detenção, de três a seis meses, ou multa”. (BRASIL, 1940, s.p.)

Logo, a apologia ao crime ou ao criminoso trata-se de fazer a apologia, ou seja, propagar, defender, estimular, elogiar: o crime ocorrido, excluindo a apologia à contravenção; ou ainda ao autor do crime. (ISHIDA, 2009, p.475)

Em ambas as condutas, cabem ressaltar que também por meio de uso de dispositivo tecnológico, os autores incitam ou estimulam as pessoas à prática de crimes. (CRESPO, 2011, p.88)

O bem jurídico tutelado para o crime de incitação ao crime é a paz pública, neste caso o sentimento de tranquilidade e segurança. (ISHIDA, 2009, p.473)

Para o crime de apologia ao crime ou ao criminoso, bem jurídico tutelado também é a paz pública, porém neste caso refere-se a segurança pública atingida. (ISHIDA, 2009, p.475)

Dentro desta tipicidade, as condutas mais comuns ocorridas são as pessoas que aderem certas comunidades, grupos de discussões e páginas de redes sociais, e que façam a interação com as mesmas, de forma que veiculem suas apologias através de mensagens como, por exemplo, de agressão a outras pessoas ou ainda relacionada a tráfico de drogas. (CRESPO, 2011, p.88)

4.2.4 Falsidade Ideológica e Falsa Identidade

A lei brasileira prevê vários crimes de falsidade, entretanto os mais comuns são os crimes de falsidade ideológica e falsa identidade respectivamente, estando estes dispostos pelo Código Penal Brasileiro através dos artigos. 299 e 307, que disciplinam respectivamente que:

> Art. 299 - Omitir, em documento público ou particular, declaração que dele devia constar, ou nele inserir ou fazer inserir declaração falsa ou diversa da que devia ser escrita, com o fim de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante: Pena - reclusão, de um a cinco anos, e multa, se o documento é público, e reclusão de um a três anos, e multa, se o documento é particular. Art. 307 - Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem: Pena - detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave.

O crime de falsidade ideológica é o ato de omitir, ou seja, deixar de inserir ou não mencionar, em documento público ou particular, declaração dissociada da realidade que neste documento deveria constar, ou ainda inserir ou fazer inserir falsa ou diversa declaração que deveria ser escrita, com o objetivo de

prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante. (NUCCI, 2011, p. 989)

Em ambos os crimes, ou seja, tanto para o crime de falsidade ideológica quanto para o crime de falsa identidade, o bem jurídico tutelado é a fé pública. (ISHIDA, 2009, p.501-512)

Tratando-se de falsidade ideológica por meio de dispositivos tecnológicos, normalmente tem-se uma inserção de dados falsos ou ainda a omissão de algo o qual deveria constar, em documentos públicos ou particulares intencionalmente com o intuito de prejudicar direito, criar obrigações ou alterar a verdade de fatos juridicamente relevante. Em outras palavras, é mentir em um documento, alterando o conteúdo deste para modificar algum tipo de direito de alguém. (CRESPO; 2011. p. 89)

No tocante a falsa identidade, Wendt e Jorge (2012, p.105) define como “ação de se atribuir ou atribuir a outra pessoa falsa identidade para obter vantagem em proveito próprio ou de outro indivíduo ou para proporcionar algum dano”.

Neste tipo de crime por meio de dispositivos tecnológicos, os casos mais comuns são de pessoas que se passam por outras pessoas para obter vantagem própria ou a terceiro, ou ainda para causar dano a outrem. (CRESPO; 2011. p. 89)

Os exemplos atuais desta modalidade são os fakes, que são pessoas que se passam por outras em redes sociais através da criação de perfis falsos em redes sociais. (CRESPO; 2011. p. 89)

4.2.5 Violação de Direitos Autorais, uso indevido de marcas, pirataria de software, concorrência desleal e espionagem eletrônica/industrial

Os crimes virtuais de violação de direitos autorais pela internet são comuns pela internet e demais dispositivos tecnológicos.

A Constituição Federal disciplina, por meio do art. 5º, inciso XXVII, que “aos autores pertence o direito exclusivo de utilização, publicação ou reprodução de

suas obras, transmissível aos herdeiros pelo tempo que a lei fixar". (BRASIL, 1988, s.p.)

Neste sentido e visando tutelar o direito autoral do autor, neste caso o bem jurídico tutelado, é que o Código Penal Brasileiro pelo texto descrito no art. 184, aborda a violação de direitos autorais como crime, ou seja, "violar direitos de autor e os que lhe são conexos" prevendo "pena de detenção, de 3 (três) meses a 1 (um) ano, ou multa". (BRASIL, 1940, s.p.)

A violação de direitos autorais é o ato de ofender ou transgredir os direitos do autor da obra intelectual ou o titular sobre a produção intelectual de outrem, como no caso de escritor de livro ou compositor de música, bem como os direitos conexos, como os da editora ou gravadora. (NUCCI, 2011, p.799)

Destarte, com relação aos crimes cometidos por meio de dispositivos tecnológicos e internet, dois são os grandes ramos: o da propriedade industrial, o qual abarca patentes, desenho industrial, marcas e nomes de domínio; e o de direitos autorais, onde este refere-se a softwares, banco de dados e documentos técnicos. (CRESPO, 2011, p.89)

A lei 9279/96 referente à Propriedade Industrial aborda a partir de seu art. 183 até o art. 195 com seus incisos e parágrafos respectivamente, os crimes contra a propriedade industrial, discorrendo sobre os seguintes crimes: contra as patentes, contra os desenhos industriais, contra as marcas, cometidos por meio de marca, título de estabelecimento e sinal de propaganda, contra indicações geográficas e demais indicações e concorrência desleal. Todos estes casos com o objetivo de proteção aos direitos autorais do autor. (BRASIL, 1996, s.p.)

No tocante ao uso indevido de marcas, os artigos 189, 190 e 191 da lei 9279/96 dão ênfase ao tema.

Disciplina o artigo 189 da lei 9279/96 que:

> Art. 189. Comete crime contra registro de marca quem: I - reproduz, sem autorização do titular, no todo ou em parte, marca registrada, ou imita-a de modo que possa induzir confusão; ou II - altera marca registrada de outrem já aposta em produto colocado no mercado. Pena - detenção, de 3 (três) meses a 1 (um) ano, ou multa. (BRASIL, 1996, s.p.)

O artigo 189 da lei 9279/96 prevê como crime contra a marca a reprodução sem autorização, a imitação que induza confusão ou a alteração da marca de outrem que já possua produto no mercado.

Já o artigo 190 da referida lei disciplina que:

> Art. 190. Comete crime contra registro de marca quem importa, exporta, vende, oferece ou expõe à venda, oculta ou tem em estoque: I - produto assinalado com marca ilicitamente reproduzida ou imitada, de outrem, no todo ou em parte; ou II - produto de sua indústria ou comércio, contido em vasilhame, recipiente ou embalagem que contenha marca legítima de outrem. Pena - detenção, de 1 (um) a 3 (três) meses, ou multa. (BRASIL, 1996, s.p.)

O artigo 190 da lei 9279/96 prevê como crime contra o registro da marca para quem importa, exporta, vende, oferece ou expõe à venda oculta ou tem em estoque: produtos irregulares no tocante a marca, ou seja, provindo de reprodução ilícita ou imitação, podendo ser somente parte do produto; ou ainda produto em sua própria indústria usando embalagens com marcas de outrem.

Por fim, o artigo 191 da referida lei disciplina que:

> Art. 191. Reproduzir ou imitar, de modo que possa induzir em erro ou confusão, armas, brasões ou distintivos oficiais nacionais, estrangeiros ou internacionais, sem a necessária autorização, no todo ou em parte, em marca, título de estabelecimento, nome comercial, insígnia ou sinal de propaganda, ou usar essas reproduções ou imitações com fins econômicos. Pena - detenção, de 1 (um) a 3 (três) meses, ou multa.Parágrafo único. Incorre na mesma pena quem vende ou expõe ou oferece à venda produtos assinalados com essas marcas. (BRASIL, 1996, s.p.)

O artigo 191 da lei 9279/96 prevê como crime contra a marca a reprodução sem autorização, a imitação que induza confusão que atinjam as armas, brasões ou distintivos oficiais nacionais, estrangeiros ou internacionais.

Logo, os crimes contra marca descritos por meio dos artigos expostos são comuns e facilitados pela internet através de sites e redes sociais, uma vez que a obtenção e o uso da marca são relativamente simples, bem como a identificação do autor é complexa.

Com relação a violação de direito autoral de software, crime no qual visa-se proteger o bem jurídico também os direitos do autor, denominada popularmente como pirataria de software, a Lei 9609/98 aborda o tema de forma a tratar como crime a violação de direitos de autor de programa de computador e atividades comerciais produzidas tendo como objeto o software violado. (CRESPO, 2011. p. 89)

A lei 9609/98, dispõe através de seu artigo 12 que comete crime a violação dos direitos do autor de programa de computador, com a punição para aquele que incorrer na conduta a pena de detenção de seis meses a dois anos ou multa. (BRASIL, 1998, s.p.)

O mesmo artigo, em seu parágrafo 1º prevê complementando o caput que se na violação citada tiver consequência de reprodução, sem autorização do autor, e que seja realizada por meio, de programa de computador, mesmo que somente em parte ou ainda na íntegra, para fins de comércio, a pena prevista é de reclusão de um a quatro anos e multa. (BRASIL, 1998, s.p.)

A pena do parágrafo 1º se estende ao parágrafo 2º do mesmo artigo 12 da lei 9609/98, para quem vender ou expor a venda, introduzir no País, adquirir, ocultar ou ter em depósito, para fins de comércio, independente se original ou cópia de programa de computador, produzido com violação de direito autoral. (BRASIL, 1998, s.p.)

No tocante a crimes contra empresas, atualmente por conta de todo o desenvolvimento tecnológico o qual permite as empresas cada vez mais facilidade e agilidade, as empresas passaram a ficar dependente de softwares, banco de dados e serviços on-line. A contrapartida da utilização da tecnologia nas atividades empresariais é a exposição aos crimes virtuais, bem como a tendência a serem visados. (CRESPO, 2011. p. 91)

Cabe ainda ressaltar que além dos crimes de violação de direitos autorais, uso indevido de marcas, pirataria de software e espionagem eletrônica, são comuns no âmbito empresarial outros crimes como pornografia infantil, a falsa identidade; todos abordados aqui abordados.

A lei 9279/96 referente à Propriedade Industrial dispõe alguns mais dos principais crimes no âmbito empresarial e cometidos por meio virtual como a concorrência desleal e a espionagem industrial.

A concorrência desleal é o tipo de conduta que tem como objetivo prejudicar a reputação ou os negócios alheios. (COELHO, 2013,p.53)

O bem jurídico tutelado neste tipo de crime é a atividade econômica presente e desenvolvida na economia livre de mercado. (NASCIMENTO, 2012, p.68)

Neste sentido, a tipificação da conduta de concorrência desleal por meio de dispositivos tecnológicos, é principalmente exposta por meio do art. 195,

inciso XI da lei 9279/96, discorrendo que comete crime de concorrência desleal aquele que:

> XI - divulga, explora ou utiliza-se, sem autorização, de conhecimentos, informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços, excluídos aqueles que sejam de conhecimento público ou que sejam evidentes para um técnico no assunto, a que teve acesso mediante relação contratual ou empregatícia, mesmo após o término do contrato; (BRASIL, 1996, s.p.)

Em outras palavras, comete o crime de concorrência desleal aquele, sem a autorização, divulgar ou explorar informações ou dados confidenciais a que teve acesso durante a relação contratual ou empregatícia mesmo após o término do vínculo, salvo se as informações ou dados já são de conhecimento público ou evidentes a especialistas.

Com relação ao crime de espionagem industrial, e no caso de espionagem industrial por meio de dispositivos tecnológicos denominada como espionagem eletrônica é, a obtenção de acesso às informações não autorizadas. (PINHEIRO; 2013, s.p.)

Quando se fala em espionagem eletrônica em sua forma, a mesma normalmente acontece no ramo empresarial e pode vir externa em caso de ataque ou então internamente, principalmente de funcionários de empresas, os quais obtém acesso às informações. (PINHEIRO; 2013, s.p.)

Não há tipificação penal específica para a conduta de espionagem eletrônica, uma vez que a mesma está tipificada por meio de alguns artigos do Código Penal Brasileiro, como os artigos 154 e 184 e também na Lei 9279/96, Lei de Propriedade Industrial, no que toca a marcas e patentes. (PINHEIRO; 2013, s.p.)

O artigo 154 do Código Penal Brasileiro disciplina que aquele que “revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem: Pena - detenção, de três meses a um ano, ou multa”. (BRASIL, 1940, s.p.)

Já o artigo 184 do Código Penal Brasileiro faz menção aquele que “violar direitos de autor e os que lhe são conexos: Pena – detenção, de 3 (três) meses a 1 (um) ano, ou multa”. (BRASIL, 1940, s.p.)

Por fim, a lei 9279/96 referente a Propriedade Industrial, aborda a espionagem industrial por meio de seu art. 195, incisos XII e XIII, os quais disciplinam que:

> Art. 195. Comete crime de concorrência desleal quem: XII - divulga, explora ou utiliza-se, sem autorização, de conhecimentos ou informações a que se refere o inciso anterior, obtidos por meios ilícitos ou a que teve acesso mediante fraude; ou XIII - vende, expõe ou oferece à venda produto, declarando ser objeto de patente depositada, ou concedida, ou de desenho industrial registrado, que não o seja, ou menciona-o, em anúncio ou papel comercial, como depositado ou patenteado, ou registrado, sem o ser; (BRASIL, 1996, s.p.)

Logo, a espionagem industrial pode impactar na concorrência deslael, principalmente nos casos citados do artigo 195, incisos XII e XIII, da lei 9279/96.

Com relação ao bem jurídico tutelado nos crimes de espionagem, no caso de espionagem eletrônica o bem jurídico tutelado é a liberdade individual e privacidade das pessoas (CABETTE, 2013, s.p.).

Neste sentido o crime de espionagem industrial, o bem jurídico a ser tutelado é também a liberdade individual, porém sob o prisma de inviolabilidade de segredo profissional. (ISHIDA, 2009, p.284)

4.2.6 Pornografia Infantil

A pornografia infantil, diga-se por meio de dispositivos tecnológicos, é segundo Wedt (2012, p.98) “uma forma ilegal de pornografia que se caracteriza pela utilização de imagens de cunho erótico de crianças e adolescentes e representa uma das maiores preocupações na internet”.

Cabe ressaltar que o artigo 2º do Estatuto da Criança e do Adolescente define como criança pessoas com até 12 anos incompletos de idade e adolescente entre 12 e 18 anos de idade. (BRASIL, 1990, s.p.)

Os principais crimes relacionados à pornografia infantil são tratados pelo artigo 240 e seguintes do Estatuto da Criança e do Adolescente, bem como pelo Código Penal Brasileiro por meio de seu artigo 217-A e outros como para casos de exploração da prostituição, dentre outros. (CRESPO; 2011. p. 90)

Destarte, a redação dada pela Lei nº 11.829, de 2008, incluiu vários dispositivos ao Estatuto da Criança e do Adolescente, o que tornou o Brasil como um dos poucos países a possuir uma legislação específica para punir a pornografia infantil por meio de computador. (WENDT;JORGE; 2012, p.98)

Na opinião de Crespo a lei brasileira abarca diversas situações que possam envolver a sexualidade:

> Ocorre que a lei brasileira pune diversas formas situações envolvendo a exposição da sexualidade infantil em fotos, imagens, filmagens e interpretações teatrais, como, por exemplo, a produção, reprodução, filmagem e o registro de cenas de sexo explícito envolvendo situações de pornografia com crianças e adolescentes. (2011, p.90)

Neste sentido, o Estatuto da Criança e do Adolescente, lei 8069/1990 atualmente dispõe por vários de seus artigos, crimes cometidos contra a criança e o adolescente, inclusive com as condutas previstas podendo ser realizadas por meio virtual, os quais expõe-se os principais a seguir.

O artigo 240 da lei 8069/1990 prevê punição de 4 a anos de reclusão para aquele tiver a conduta de produzir, reproduzir, dirigir, fotografar, filmar ou registrar, independente do meio utilizado, cena de sexo explícito ou pornográfica que envolva criança ou adolescente. (BRASIL, 1990, s.p.)

A mesma pena do caput do artigo 240 da lei 8069/90, aplica-se nos casos previstos no parágrafo primeiro do mesmo artigo para aquele que agenciar, recrutar, coagir ou intermediar a participação da criança ou do adolescente em cenas de sexo explícito ou pornográficas ou contracenando nestas cenas. (BRASIL, 1990, s.p.)

A pena aumenta em um terço do previsto no caput do artigo 240 da lei 8069/1990, previsão do parágrafo segundo do mesmo artigo em seus inicisos, para os casos em que sejam cometidos por funcionário público; pelos que possuírem relações domésticas, de coabitação ou ainda de hospitalidade; por parentes de sangue até 3º grau, ou ainda por adoção, tutor, curador, preceptor, empregador da vítima ou de quem tenha autoridade sobre esta. (BRASIL, 1990, s.p.)

Já o artigo 241 da lei 8069/90 dispõe sobre a comercialização ou exposição de vídeo, foto e outros registros que contenha cena de sexo explícito ou pornográfica que contenham criança ou adolescente, com previsão de pena de reclusão de quatro a oito anos. (BRASIL, 1990, s.p.)

O artigo 241-A da lei 8069/90 prevê condutas como oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar vídeo, fotografia ou outra forma de registro, contendo cenas de sexo explícito ou pornográfica que envolvam crianças ou adolescentes. Cabe destacar neste artigo que o mesmo faz menção para o meio por onde é realizada a conduta, ressaltando que inclusive as condutas realizadas por meio de sistema de informática ou telemático. A pena prevista para este crime é de reclusão de 3 a 6 anos e multa. (BRASIL, 1990, s.p.)

O artigo 241-B da lei 8069/90 prevê punição de reclusão de 1 a 4 anos e multa para aquele que realizar as condutas de adquirir, possuir ou armazenar, vídeos, fotografias ou outra forma de registro, independente do meio pelo qual obtenha-os, e que contenham criança ou adolescente. (BRASIL, 1990, s.p.)

Caso a quantidade do material seja pequena, a pena prevista no caput do artigo 241-B poderá ser diminuída de 1 a 2/3, conforme o parágrafo primeiro do referido artigo. (BRASIL, 1990, s.p.)

Importante ressaltar que não há crime nos casos de posse ou armazenamento de cenas de sexo explícito ou pornográficas, por agente público no exercício de sua função, por membro de entidade que noticiam crimes ou por representante legal e funcionários de provedor de acesso à internet, com a finalidade de comunicação as autoridades competentes, inclusive cabendo aos mesmos manter em sigilo o material. (BRASIL, 1990, s.p.)

O artigo 241-C da lei 8069/90 refere-se à simulação de cenas de sexo explícito ou pornográficas incluindo participação de crianças ou adolescentes, por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação. A pena para quem incorre neste tipo de conduta é de 1 a 3 anos de reclusão. (BRASIL, 1990, s.p.)

Já o artigo 241-D da lei 8069/90 atinge as condutas de aliciamento, assédio, instigação e constrangimento a criança com a finalidade de que esta pratique ato libidinoso. A pena prevista para este tipo de crime é de 1 a 3 anos, e multa. (BRASIL, 1990, s.p.)

Ainda sobre o artigo 241-D, os seus incisos I e preveem a aplicação da mesma pena para aquele facilita ou induz o acesso à criança de material que contenha cenas de sexo explícito ou pornográficas com a finalidade de que esta pratique ato libidinoso, ou ainda aquele pratica as condutas descritas no caput com a

finalidade de induzir a criança a se exibir pornograficamente ou sexualmente explícita. (BRASIL, 1990, s.p.)

Por fim, o artigo 241-E da lei 8069/90 complementa os artigos anteriores a este, definindo a expressão sexo explícito ou pornográfica como “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”. (BRASIL, 1990, s.p.)

Logo, o Estatuto da Criança e do Adolescente, por meio dos artigo apresentados é a principal tipificação dos crimes contra a criança e o adolescente, tentado abarcar o máximo de condutas possíveis a serem realizadas, inclusive virtualmente.

Neste sentido, pode-se ver também a ação dos tribunais através de uma das decisões do Tribunal Regional Federal da 4ª Região acerca do tema:

> PENAL. PROCESSUAL PENAL. HABEAS CORPUS. PEDOFILIA. ART. 241 DA LEI 8.069/90. ECA. PRISÃO PREVENTIVA. GARANTIA DA ORDEM PÚBLICA. ORDEM DENEGADA. 1. Na hipótese dos autos que trata do crime do art. 241 da Lei 8.069/90, para enfrentamento de pedido de prisão preventiva ou concessão e liberdade, não basta a constatação dos requisitos tradicionais, tais como, como a ausência de antecedentes, endereço fixo e profissão lícita, isto porque o conceito de ordem pública ganha novos contornos, devendo ser analisada à luz das determinações constitucionais de proteção à criança e ao adolescente. [...] 3. A gravidade do delito atribuído ao paciente é indiscutível, na medida em que para a produção das imagens disseminadas pela rede mundial de computadores é indispensável que crianças e adolescentes sejam objeto de abuso sexual e outras sevícias, sem o quê as mídias não existiriam. Por conseguinte, a divulgação destas mídias, muitas vezes mediante pagamento, além de constituir-se em crime autônomo é forma de manutenção da atividade criminosa que necessariamente a antecede. 4. O fato de tratar-se de delito praticado sub-repticiamente no chamado "mundo virtual" pode, à primeira vista, mascarar o efetivo alcance das nocivas conseqüências do crime perpetrado. Veja-se, conforme noticiado, foram localizados "em apenas 12 dias, mais de 100 vídeos e 10.000 fotografias com imagens de pedofilia, disponibilizados por mais de 13.000 usuários da rede Emule". [...] Ordem denegada. (TRF-4 - HC: 41106 SC 2008.04.00.041106-0, Relator: GERSON LUIZ ROCHA, Data de Julgamento: 02/12/2008, SÉTIMA TURMA, Data de Publicação: D.E. 07/01/2009)

Já o Código Penal Brasileiro, o qual foi editado pela lei 12.015 de 2009, aborda o tema, principalmente por intermédio de seus artigos 217-A e 218-B.

O artigo 217-A do Código Penal Brasileiro disciplina que “ter conjunção carnal ou praticar outro ato libidinoso com menor de 14 (catorze) anos”, com pena prevista de reclusão de 8 (oito) a 15 (quinze) anos. (BRASIL, 1940, s.p.)

O artigo 218-B do Código Penal Brasileiro dispõe que:

> Art. 218-B. Submeter, induzir ou atrair à prostituição ou outra forma de exploração sexual alguém menor de 18 (dezoito) anos ou que, por enfermidade ou deficiência mental, não tem o necessário discernimento para a prática do ato, facilitá-la, impedir ou dificultar que a abandone: Pena - reclusão, de 4 (quatro) a 10 (dez) anos. (BRASIL, 1940, s.p.)

Este artigo faz menção principalmente à prostituição e a exploração sexual, no sentido de induzir ou submeter ao menor de 18 anos ou aquele que possua enfermidade ou deficiência mental, ou seja, que não tenha discernimento para a prática do ato.

Importante salientar que nos crimes de pornografia infantil e seus respectivos dispositivos, o bem jurídico tutelado principal é a proteção à liberdade sexual, inclusive no aspecto moral. (NUCCI, 2011, p.847)

Por fim, a pornografia infantil como crime virtual é um tema que apesar de toda a tipificação disposta no ordenamento jurídico brasileiro, é de extrema complexidade principalmente no tocante ao controle de distribuição do conteúdo como fotos e vídeos

4.2.7 Crimes contra a Honra

A honra é, no entendimento de Crespo (2012, p.90), “qualidades físicas, morais e intelectuais de uma pessoa, importando sua aceitação ou rejeição social”.

Neste mesmo sentido, Ishida (2009, p.256) ressalta que a honra é “conjunto de atributos morais, intelectuais e físicos de uma pessoa, que lhe conferem consideração social e estima própria”.

No tocante a honra, a mesma pode ser dividida em dois tipos, sendo estes a honra subjetiva que é o sentimento de cada um perante seus atributos físicos, intelectuais, sociais e morais, e a honra objetiva que trata-se do juízo que a comunidade faz do indivíduo. (ISHIDA; 2009, p.256)

Os crimes contra a honra estão entre os mais comuns da internet. Os mesmos estão previstos no Código Penal Brasileiro, por meio dos artigos 138, 139 e

140, os quais abordam respectivamente os crimes de calúnia, difamação e injúria. (CRESPO, 2012. p.90)

> Esses crimes que se alastram com extrema facilidade com o uso da internet se tornaram ainda mais evidente com o advento das novas tecnologias, se expressar manifestar uma opinião, com ilustrações como vídeo, foto, mensagens com áudio etc. Com a criação de blogs, sites de relacionamento dentre outras maneiras ofender e ser ofendido, seja direta ou indiretamente acabou se tornando rotina na vida de quem acessa a grande rede.- grave.(GATTO, 2011, [s.p.])

A calúnia é o ato de afirmar que a vítima cometeu um fato criminoso. (WENDT;JORGE, 2011, p.103)

Destarte, este tipo de crime atribui um fato criminoso a vítima por meio de uma acusação que se sabe ser falsa, ou seja, o criminoso deve saber que trata-se de fato falso. (CRESPO, 2012, p.90)

Caluniar é fazer uma acusação falsa, tirando a credibilidade de uma pessoa no seio social e assim ferindo a honra objetiva da vítima perante terceiros. (NUCCI, 2011, p.689)

O bem jurídico tutelado no crime de calúnia é a honra objetiva, ou seja, a reputação perante a sociedade ou ao meio social no qual convive. (ISHIDA, 2009, p.256)

A calúnia está prevista através do art. 138 do Código Penal Brasileiro, o qual discorre que “caluniar alguém, imputando-lhe falsamente fato definido como crime”, prevendo pena de detenção de seis meses a dois anos. (BRASIL, 1940, s.p.)

Um exemplo comum de calúnia por meio de internet e dispositivos tecnológicos pode ser dado em caso onde um usuário de rede social ou de softwares de comunicação instantânea, espalha e-mails ou divulga em redes sociais ou softwares de comunicação instantânea que determinada pessoa desviou quantias de dinheiro. (WENDT;JORGE, 2011, p.103)

A difamação é o ato de propagar fatos que sejam ofensivos que toquem a reputação da vítima. (WENDT;JORGE, 2011, p.103)

Neste mesmo sentido, Crespo (2012, p.91) enfatiza que “a difamação é a atribuição de fato ofensivo à reputação de alguém, desacreditando-a publicamente”.

Difamar é desacreditar publicamente uma pessoa, maculando-lhe a reputação, atingindo sua honra objetiva. (NUCCI, 2011, p.692)

Na difamação, assim como no crime de calúnia, o bem jurídico tutelado é a honra objetiva, ou seja, a reputação perante a sociedade ou ao meio social no qual convive. (ISHIDA, 2009, p.259)

A difamação está prevista através do art. 139 do Código Penal Brasileiro, o qual discorre que “difamar alguém, imputando-lhe fato ofensivo à sua reputação”, prevendo pena de detenção de três meses a um ano e multa. (BRASIL, 1940, s.p.)

Cabe ressaltar que na difamação, a atribuição do fato deve ser específica, porém caso este fato seja considerado crime, não há a difamação e sim calúnia. Ainda ressalta-se que ambos os crimes somente se consumam quando uma terceira pessoa toma conhecimento do fato. (CRESPO, 2012, p.91)

Um exemplo comum de difamação por meio de internet e dispositivos tecnológicos pode ser dado em caso onde um usuário de rede social ou de softwares de comunicação instantânea, divulga algum caso extraconjugal de um terceiro a outras pessoas, onde independente da veracidade do fato, a reputação da vítima foi prejudicada. (CRESPO, 2012, p.91)

A injúria é o ato ofender a dignidade ou decoro de outras pessoas, e está normalmente relacionado a xingamentos. (WENDT;JORGE, 2011, p.103)

Neste tipo de crime não há atribuição de fato a alguém, porém há a atribuição de características negativas sobre as qualidades físicas, morais ou intelectuais da vítima, como ofensas, insultos, dentre outros, violando assim a honra subjetiva do sujeito. (CRESPO, 2012, p.91)

Para Nucci (2011, p.694) não basta ofender ou insultar, “é preciso que a ofensa atinja a dignidade ou decoro de alguém”.

Diferente dos crimes de calúnia e de difamação, o crime de injúria tem como bem jurídico tutelado a honra subjetiva da pessoa, ou seja, a honra enquanto dignidade, enquanto sentimento que cada pessoa sente a respeito de seus atributos físicos, intelectuais, sociais ou morais. (ISHIDA, 2009, p.262)

A injúria está prevista através do art. 140 do Código Penal Brasileiro, o qual discorre que “injuriar alguém, ofendendo-lhe a dignidade ou o decoro”, prevendo pena de detenção de um a seis meses, ou multa. (BRASIL, 1940, s.p.)

Um exemplo comum de injúria por meio de internet e dispositivos tecnológicos pode ser dado em caso onde a pessoa filma a vítima sendo agredida

ou humilhada e divulga em rede social, por meio de softwares de comunicação instantânea ou ainda em sites específicos de vídeos. (WENDT;JORGE, 2011, p.103)

Ainda no tocante a crimes contra a honra e a injuria, uma das espécies de maior repercussão ocorridas no Brasil por meio de internet e dispositivos tecnológicos é a injúria racial. (WENDT;JORGE, 2011, p.101)

Este crime foi introduzido pela Lei 9.459/97 com o objetivo de evitar as absolvições que vinham ocorrendo nos casos em que pessoas ofendiam outras, através de insultos raciais ou discriminatórios e escapavam da lei 7.716/89 que disciplina especificamente a discriminação racial e quando muito, respondiam por injúria descrita no caput do art. 140. (NUCCI, 2011, p.696)

Para o Ministério Público do Distrito Federal e Territórios (s.d, s.p.), a injúria racial "consiste em ofender a honra de alguém com a utilização de elementos referentes a raça, cor, religião ou origem".

Tal conduta está tipificada através do texto do parágrafo 3º do art. 140 da Lei 9.459/97, o qual discorre que "se a injúria consiste na utilização de elementos referentes a raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência" com pena prevista para reclusão de um a três anos e multa.

Destarte, enfatiza-se que:

> Assim, aquele que atualmente, dirige-se a uma pessoa de determinada raça, insultando-a com argumentos ou palavras de conteúdo pejorativo, responderá por injúria racial, nãopodendo alegar que houve uma injúria simples, nem tampouco uma mera exposição de pensamento, uma vez que há limite para tal liberdade. (NUCCI, 2011, p.696)

Por fim, cabe ressaltar que grande parte das ocorrências de crimes contra a honra por meio de internet e dispositivos tecnológicos são os cometidos em publicações de redes sociais, softwares de comunicação instantânea, e-mails e sites. (CRESPO, 2012, p.91)

Neste sentido ainda, é importante frisar que incorre na mesma conduta a pessoa que divulga a publicação. (CRESPO, 2012, p.91)

Acerca do tema, o Tribunal de Justiça do Estado do Paraná apresenta uma de suas decisões com o seguinte texto:

> DECISÃO: ACORDAM os Magistrados integrantes da Segunda Câmara Criminal do Egrégio Tribunal de Justiça do Paraná, à unanimidade, em dar

> parcial provimento ao recurso. EMENTA: RECURSO EM SENTIDO ESTRITO. CRIMES CONTRA A HONRA PRATICADOS PELA INTERNET (FACEBOOK). QUEIXA-CRIME RECEBIDA APENAS PELO CRIME DE INJÚRIA. PLEITO DE RECEBIMENTO PELOS CRIMES DE CALÚNIA E DIFAMAÇÃO. CALÚNIA NÃO CARACTERIZADA.FATOS QUE SE REFEREM A TERCEIRA PESSOA E NÃO AO QUERELANTE. AFASTAMENTO.DIFAMAÇÃO. OFENSA À HONRA OBJETIVA (REPUTAÇÃO) DO QUERELANTE. CONDUTA QUE NÃO CONFIGURA BIS IN IDEM COM O CRIME DE INJÚRIA. BENS JURÍDICOS DISTINTOS. RECURSO PARCIALMENTE PROVIDO. "Ainda que diversas ofensas tenham sido assacadas por meio de uma única carta, a simples imputação à acusada dos crimes de calúnia, injúria e difamação não caracteriza ofensa ao princípio que proíbe o bis in idem, já que os crimes previstos nos artigos 138, 139 e 140 do Código Penal tutelam bens jurídicos distintos, não se podendo asseverar de antemão que o primeiro absorveria os demais" (RHC 41.527/RJ, Rel. Ministro JORGE MUSSI, QUINTA TURMA, julgado em 03/03/2015, DJe 11/03/2015). I. (TJPR - 2ª C.Criminal - RSE - 1462862-5 - Jaguariaíva - Rel.: José Mauricio Pinto de Almeida - Unânime - - J. 25.02.2016) (TJ-PR - RSE: 14628625 PR 1462862-5 (Acórdão), Relator: José Mauricio Pinto de Almeida, Data de Julgamento: 25/02/2016, 2ª Câmara Criminal, Data de Publicação: DJ: 1765 22/03/2016)

O julgado acima exposto dá provimento parcial a recurso de sentido estrito no caso em que há o cometimento de um dos crimes contra a honra, neste caso o crime de injúria, inclusive com indeferimento dos crimes de calúnia e difamação, requeridos pelo querelante do caso. O julgado em questão relata cometimento do crime por meio de uma rede social.

4.2.7.1 Cyberbullying

O bullying pode ser definido como atitudes de natureza agressivas, intencionais e repetitivas as quais são tomadas por uma única pessoa ou por um determinado grupo de pessoas em face à outra pessoa, causando a esta dor, angustia e sofrimento. (ALBINO;TERENCIO, s.d; p.1)

Estas atitudes normalmente são tomadas em situação de desvantagem de poder do autor perante a vítima dificultando a esta a defesa. (ALBINO;TERENCIO, s.d; p.1)

Para Fiorillo e Conte (2016, p.256) a prática do bullying aborda “atos premeditados e repetidos de violência física ou psicológica praticados para intimidar ou agredir alguém”.

Neste diapasão, surge o cyberbullying, termo que denomina uma variação do bullying, ou seja, é o mesmo tipo de atitude, porém praticada por intermédio de dispositivos tecnológicos, bem como por internet. (WENDT;JORGE; 2011, p.102)

Neste sentido, a ofensa toma uma dimensão muito maior do que o normal, uma vez que a rápida disseminação pela rede mundial de computadores permite em pouco tempo a disponibilização a uma infinidade de locais e consequentemente acessos aos inúmeros usuários. (WENDT;JORGE; 2011, p.102)

Destarte, o cyberbullying busca atingir a vítima no aspecto psicológico, normalmente os corridos por meio de fóruns-online através de grupos de discussões, blogs, salas de bate-papo, e-mails, mensagens instantâneas, serviços de mensagens breves via celular, smartphones, sites de relacionamentos, dentre outros. (FIORILLO;CONTE, 2016, p.257)

No tocante a tipificação penal do cyberbullying, não há uma específica prevista no ordenamento jurídico, porém a conduta pode gerar reflexos que podem ser enquadrados no Código Penal Brasileiro, principalmente entre os artigos 138 e 145 onde são previstos os crimes contra a honra. (CASADO; 2011, [s.p.])

Cabe ressaltar ainda que a lei 13.185/2015 institui o Programa de Combate a Intimidação Sistemática (Bullying) em todo o território nacional, com os objetivos principais de combater e prevenir as condutas, bem como de assistir vítimas. (BRASIL; 2015, s.p.)

No tocante ao cyberbullying, o parágrafo 2º, além de prever todas as condutas abarcadas pelo bullying e o parágrafo único que disciplina sobre as mesmas condutas, porém realizadas na internet:

> Art. 2o Caracteriza-se a intimidação sistemática (bullying) quando há violência física ou psicológica em atos de intimidação, humilhação ou discriminação e, ainda: I - ataques físicos; II - insultos pessoais; III - comentários sistemáticos e apelidos pejorativos; IV - ameaças por quaisquer meios; V - grafites depreciativos; VI - expressões preconceituosas; VII - isolamento social consciente e premeditado; VIII - pilhérias. (BRASIL; 2015, s.p.)

Logo, o que busca-se é identificar as condutas do bullying realizadas por meio da internet, caracterizadas como cyberbullying, principalmente quando a violência é psicológica, humilhação, discriminação e preconceito, ameaças, apelidos pejorativos, ou ainda outras formas que exponham de forma atingir a moral e a

estima, e assim poder combater e prevenir, de forma que não permita mais o cometimento destas condutas.

Cabe destacar o parágrafo único do artigo 2º da lei 13185/2015, o qual enfatiza especificamente sobre tais condutas previstas no caput quando são realizadas por meio de internet.

Por fim, trata-se de um tema este que esta em voga na sociedade contemporânea atualmente e que deve ser tratado de forma minuciosa, uma vez que toca diretamente disposições físicas, psicológicas e morais das pessoas, o que necessita atenção por parte das autoridades, principalmente nas consequências geradas por tais condutas.

4.2.8 Fraudes Virtuais (Furto, Estelionato e Fraudes)

A fraude, segundo Guimarães (2012, p.128) é um “artifício malicioso, usado para prejudicar, dolosamente, o direito ou interesses de terceiros”.

Neste mesmo sentido, conceitua-se ainda de forma ampla a fraude como um esquema criado e usado para obter ganhos pessoais. (WENDT;JORGE, 2012, p.74)

Para Pinheiro (2013, s.p.) “toda fraude, independente de sua natureza, tem como pressuposto a utilização de um subterfúgio para ludibriar a vítima, seja por meio da ação ou da omissão do agente”.

Neste sentido, cabe ressaltar que o bem jurídico tutelado nestes tipos de crimes são o patrimônio e a moralidade do comércio e das relações comerciais. (ISHIDA, 2009, p.338)

A fraude pode ocorrer em vários ambientes, entretanto com o surgimento de dispositivos tecnológicos e da internet ficou potencializada a disseminação e o uso de fraudes virtuais. (WENDT;JORGE, 2012, p.75)

Destarte, é possível compreender a fraude virtual ou eletrônica, ou seja, a fraude realizada por meio de algum tipo de dispositivo tecnológico ou pela internet, da seguinte forma:

> A fraude eletrônica consiste em uma mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco,

> empresa ou site popular, e procura induzir usuários ao fornecimento de dados pessoais e financeiros. Inicialmente, esse tipo de mensagem induzia o usuário ao acesso a páginas fraudulentas na Internet. (CENTRO DE ESTUDOS, RESPOSTAS E TRATAMENTOS; [s.d.], [s.p.] apud PINHEIRO, 2013, s.p.)

Em outras palavras, conforme o conceito acima, fraude eletrônica ou virtual é uma mensagem que induz o receptor a informar dados e prestar informações para o gerador da mensagem por usufruir dos mesmos afim de fraudar.

O mesmo termo também trata da indução do receptor da mensagem que busca capturar informações prestadas pelo receptor, ainda que seja por meio de induzi-lo a instalação de códigos maliciosos. (CENTRO DE ESTUDOS, RESPOSTAS E TRATAMENTOS; [s.d.], [s.p.] apud PINHEIRO, 2013, s.p.)

A fraude virtual é classificada em duas espécies: a primeira denominada como fraude interna, é aquela em que é praticada por empregado ou terceiro, estando estes dentro do local fraudado; e a segunda denominada fraude externa na qual o fraudador não possui vinculo algum com o local fraudado. (PINHEIRO, 2013, s.p.)

Cabe ressaltar ainda que são várias as possibilidades de fraude por meio virtual, entretanto as principais encontram-se dispostas através dos artigos 171, referente ao estelionato; o artigos 175 que refere-se a fraude no comércio e neste caso o comércio virtual. (WENDT;JORGE, 2012, p.75)

No tocante ao estelionato, o art. 171 do Código Penal Brasileiro discorre que: “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”, com previsão de pena de reclusão de um a cinco anos e multa. (BRASIL; 1940, s.p.)

Na aplicação do estelionato por meio de dispositivos tecnológicos e internet, a conduta do sujeito será de levar, induzir ou manter a vítima em erro, para que se possa obter vantagem ilicitamente, podendo ser para si ou para outrem. (PAIVA, 2012, p.21)

Com relação à fraude virtual no comércio virtual, também conhecido como e-commerce, são as fraudes que envolvem as pessoas que realizam compras pela internet, em sites que são criados com a única finalidade de fraudar, onde a vítima realiza o pagamento, mas não recebe a mercadoria prometida. (WENDT;JORGE, 2012, p.76)

A previsão para este tipo de crime é apresentada pelo Código Penal Brasileiro, por meio do art. 175, o qual disciplina que:

> Art. 175 - Enganar, no exercício de atividade comercial, o adquirente ou consumidor: I - vendendo, como verdadeira ou perfeita, mercadoria falsificada ou deteriorada; II - entregando uma mercadoria por outra: Pena - detenção, de seis meses a dois anos, ou multa. (BRASIL; 1940, s.p.)

Ainda há de se ressaltar, no tocante a fraudes, a respeito de das fraudes bancárias, normalmente provindas de operação de criminosos que atuam para capturar, virtualmente ou não, os dados bancários dos clientes e agem junto ao banco para a realização de operações bancárias, como se fora o próprio cliente. (WENDT;JORGE, 2012, p.92)

Neste sentido cabe ressaltar que a maioria dos casos em que ocorre este tipo de conduta envolvendo entes financeiros o resultado é o furto, conforme disciplina o artigo 155 do Código Penal Brasileiro “Subtrair, para si ou para outrem, coisa alheia móvel”. (BRASIL; 1940, s.p.)

Em alguns casos inclusive, cabe a qualificação do furto, conforme disposto no parágrafo 4º e seus incisos, do artigo 155 do Código Penal Brasileiro, como pode-se ver em uma das decisões Tribunal Regional Federal da 4ª Região:

> PENAL E PROCESSO PENAL. HABEAS CORPUS. CONDENAÇÃO POR FURTO QUALIFICADO MEDIANTE FRAUDE. ART. 155, § 4º, II, DO CÓDIGO PENAL. SUBTRAÇÃO DE VALORES DE CONTA BANCÁRIA. TRANSFERÊNCIAS VIA INTERNET. DESCLASSIFICAÇÃO DA CONDUTA. ART. 154-A DO CÓDIGO PENAL. INVASÃO DE COMPUTADOR. INCABIMENTO. 1. A subtração de valores de conta bancária, mediante transferência fraudulenta via internet, sem o consentimento do correntista, configura o crime de furto qualificado, previsto no art. 155, § 4º, II, do Código Penal, sendo improcedente a pretensão de desclassificar o fato para o delito de invasão de dispositivo informático, previsto no art. 154-A do Código Penal, incluído pela Lei nº 12.737, de 2012. 2. Hipótese que não configura aplicação de lei posterior mais benéfica, pois a nova lei, invocada na impetração, já estava em vigor na data da prolação da sentença condenatória e do acórdão que a manteve. (TRF-4 - HC: 50213979020144040000 5021397-90.2014.404.0000, Relator: MÁRCIO ANTÔNIO ROCHA, Data de Julgamento: 16/09/2014, SÉTIMA TURMA, Data de Publicação: D.E. 17/09/2014)anos, ou multa.

Acerca do julgado apresentado, o que pode-se verificar é a tentativa de impetração de um Habeas Corpus a favor do acusado que supostamente tenha cometido um crime de fraude, sendo este um furto qualificado via internet, subtraindo valores de conta bancária de outrem.

Isto posto, conclui-se que as fraudes por meios virtuais comprem a mesma finalidade das condutas que não são por meio de algum dispositivo tecnológico o que tão logo permite a aplicação dos mesmos dispositivos previsto no Código Penal Brasileiro.

4.2.9 Tráfico de Drogas e Armas

O tráfico de drogas e de armas, assim como além de seus meios tradicionais, também podem ser praticado por meio de internet, uma vez que esta surge como um meio efetivo de praticar o crime, redução de custos, otimização de decisões e uma opção melhor de logística . (PINHEIRO, 2013, s.p.)

O bem jurídico tutelado pela lei penal, segundo a lei 11.343/2006, é a saúde pública. (CAPEZ, 2014, p.685)

A forma mais comum como se dão estas vendas pela internet é por meio de sites da Deep Web (internet profunda), cujo conteúdo está fora do alcance de qualquer usuário comum, funcionando como se fora um submundo oculto de usuários comuns, porém dentro da própria internet. (ORRICO, 2014, s.p.)

Além disso, o acesso a internet profunda é dado por meio de software específico e o pagamento é feito por moeda virtual própria, específica da internet chamada de Bitcoin. (ORRICO, 2014, s.p.)

A lei nº 11.343/2006, denominada como “Lei de Drogas”, prevê por meio de seus artigos, principalmente o artigo 33, o tráfico de drogas, disciplinando que:

> Art. 33. Importar, exportar, remeter, preparar, produzir, fabricar, adquirir, vender, expor à venda, oferecer, ter em depósito, transportar, trazer consigo, guardar, prescrever, ministrar, entregar a consumo ou fornecer drogas, ainda que gratuitamente, sem autorização ou em desacordo com determinação legal ou regulamentar: Pena - reclusão de 5 (cinco) a 15 (quinze) anos e pagamento de 500 (quinhentos) a 1.500 (mil e quinhentos) dias-multa. (BRASIL, 2006, s.p.)

É possível ilustrar o tráfico de drogas pela internet também através de uma das decisões do Superior Tribunal de Justiça:

> PENAL. TRÁFICO. PENA-BASE. EXASPERAÇÃO. LEGALIDADE. NATUREZA E GRANDE QUANTIDADE DA DROGA APREENDIDA. DEDICAÇÃO À ATIVIDADECRIMINOSA. CAUSA ESPECIAL DE DIMINUIÇÃO. NÃO INCIDÊNCIA. 1. Tendo sido apreendida grande quantidade de drogas (300 pontos de LSD), legitimada está a exasperação da pena-base, conforme,inclusive, os ditames do art. 42 da Lei nº 11.343/2006.2. Demonstrado pelas instâncias ordinárias que o paciente se dedica à atividade criminosa, pois, além do montante da substância entorpecente que estava na sua posse, por ocasião do flagrante, a oferecia pela internet, sem o menor pudor, realizando a transação nas proximidades de uma escola e de um hospital, não tem direito à diminuição do art. 33, § 4º da Lei nº 11.343/2006. Conclusão indene ao crivo do habeas corpus, pois demanda revolvimento fático-probatório, não condizente com o seu angusto veio desconhecimento. Precedentes.3. Ordem denegada. (STJ - HC: 176495 SP 2010/0110987-0, Relator: Ministra MARIA THEREZA DE ASSIS MOURA, Data de Julgamento: 21/06/2011, T6 - SEXTA TURMA, Data de Publicação: DJe 14/09/2011)

O que pode-se verificar é que o julgado apresenta a conduta de oferecer a droga pela internet, o que qualifica no artigo 33, parágrafo 4º da lei 11.343/2006, lei de drogas, o que dispõe sobre a diminuição da punição para o acusado que seja réu primário, tenha bons antecedentes e não se dedique a vida criminosa.

Já o bem jurídico tutelado nos crimes de tráfico de armas, segundo Capez (2014, p.355) é “a incolumidade pública, ou seja, a garantia e preservação do estado de segurança, integridade corporal, vida, saúde e patrimônio dos cidadãos indefinidamente considerados contra possíveis atos que os exponham a perigo”.

No tocante ao tráfico de armas, a lei nº 10.826/2003, disciplina a proibição do comércio de armas através do artigo 17, discorrendo que:

> Art. 17. Adquirir, alugar, receber, transportar, conduzir, ocultar, ter em depósito, desmontar, montar, remontar, adulterar, vender, expor à venda, ou de qualquer forma utilizar, em proveito próprio ou alheio, no exercício de atividade comercial ou industrial, arma de fogo, acessório ou munição, sem autorização ou em desacordo com determinação legal ou regulamentar: (BRASIL, 2003, s.p.)

Logo, o tráfico de armas que é tipificado por lei específica, também pode ser realizado pela internet, uma vez que o comércio, mesmo que de forma não tão simples ou comum, pode ser realizado.

Por fim, cabe ressaltar que apesar da tipificação penal, bem como o monitoramento de autoridades, tanto o tráfico de drogas como o tráfico de armas podem ser realizados via internet.

4.2.10 Atentado a Serviço de Utilidade Pública

Os crimes de atentado a serviço público, segundo Ishida (2009, p.444) são crimes cometidos contra os serviços públicos com o objetivo de "perturbar, atrapalhar, criando risco (segurança) ou dificultando, paralisando o funcionamento".

Os serviços disponibilizados na internet são considerados também como serviços de utilidade pública, ou seja, tem o mesmo objetivo de servir a população. (WENDT;JORGE, 2012, p.28)

O Código Penal Brasileiro, através de seu art. 265, disciplina que "Atentar contra a segurança ou o funcionamento de serviço de água, luz, força ou calor, ou qualquer outro de utilidade pública", prevendo como pena a reclusão, de um a cinco anos, e multa. (BRASIL, 1940, s.p.)

Cabe ressaltar ainda o artigo 266, bem como o seu artigo primeiro, os quais doutrinam sobre a interrupção ou perturbação dos serviços de utilidade pública relacionados a comunicação, com a seguinte redação:

> Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento: Pena - detenção, de um a três anos, e multa. § 1o Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento. dias-multa. (BRASIL, 1940, s.p.)

Em ambos os tipos, o bem jurídico tutelado é a incolumidade pública, em específico a segurança dos meios de comunicação, transportes e outros serviços públicos. (NUCCI, 2011, p.931)

5 SUJEITOS DOS CRIMES VIRTUAIS

Os sujeitos do crime são aqueles quem tem participação direta no crime, ou seja, aquele que comete a conduta e aquele tem o bem jurídico atingido por esta conduta.

Logo, serão objetos de estudo deste capítulo a seguir.

5.1 SUJEITO ATIVO

Inicialmente é importante destacar o conceito geral de sujeito ativo do crime.

O sujeito ativo da conduta típica é a pessoa humana que realiza a prática de conduta típica descrita em lei, podendo ser de forma isolada ou ainda em de forma conjunta a outros autores, abrangendo inclusive aquele que de alguma forma colabora indiretamente para a ação criminosa. (CAPEZ, 2005, p.140)

Logo, o sujeito ativo de um crime é quem pratica, de forma total ou parcial, o fato definido como crime conforme a norma penal incriminadora. (BITENCOURT, 2007, p.230)

Neste mesmo sentido, Ishida (2009, p.52) resume que o sujeito ativo do crime “é aquele quem pratica o fato típico”.

Isto posto, nos crimes virtuais tem-se algumas especificidades em relação aos demais crimes por conta de envolverem internet e dispositivos tecnológicos, e principalmente pelo fato do agente criminoso utilizar-se plenamente de seu intelecto e de seu conhecimento técnico, o que acaba trazendo uma certa peculiaridade na conduta dos criminosos. (NETO, 2005, p.267)

Neste diapasão, os sujeitos ativos, ou seja, aqueles que cometem os crimes virtuais são sujeitos que possuem um perfil diferenciado e específico, principalmente com relação ao grande conhecimento técnico de dispositivos tecnológicos e sistemas, como pode ser visto a seguir. (ORRIGO;FILGUEIRA, 2016, p.5)

Os Hackers são os chamados “piratas” do computador, ou ainda de fuçadores de computadores, pois são estes sujeitos que detém um grande conhecimento técnico sobre dispositivos tecnológicos e que em suas ações invadem sistemas para benefício próprio, com o fim de obter dados ou informações de outrem. (CRESPO, 2011, p.95)

O objetivo do Hacker a invasão de um sistema para benefício próprio, mas não cometendo condutas delituosas, criando novos programas e utilizando suas habilidades para dar sequência em programas. (MEDEIROS, 2015, s.p.)

Complementa ainda Orrigo e Filgueira (2016, p.6) disciplinando que “os Hackers utilizam de seus conhecimentos técnicos para ações lícitas”.

Já para Carneiro (2012, s.p.) “hacker é apenas um gênero e as espécies de hackers podem variar de acordo com as práticas”.

Os Crackers são sujeitos que são considerados como reais criminosos devido à má intenção que obtêm para a invasão de dispositivos e a destruição. (CRESPO, 2011, p.96)

Neste sentido, os crackers são sujeitos que buscam visibilidade e que se divertem fazendo mal, como o roubo de dinheiro e de informações pela internet, o vandalismo como pichação a sites e quebra de sistemas de segurança. (CRESPO, 2011, p.96)

Orrigo e Filgueira (2016, p.6) definem crackers como “pessoas com conhecimentos e habilidades equivalentes aos dos hackers, porém com fins ilícitos”.

O cracker seria o expert que utiliza de suas habilidades técnicas para provar prejuízo alheio, principalmente invadindo sistemas com a quebra da segurança. (MEDEIROS, 2015, s.p.)

A diferença entre hacker e cracker pode é exposta por Carneiro (2012, s.p.) da seguinte forma:

> Os hackers e os crackers geralmente são muito parecidos em relação ao vasto conhecimento aprofundado em informática e a principal distinção é a finalidade que suas praticas resultam, sendo que os hackers realizam atividades positivas, não criminosas, enquanto a motivação dos crackers é criminosa em sua essência agindo normalmente premeditadamente com objetivo criminoso de obter vantagens ilícitas.

Logo, pode-se dizer que o hacker é aquele que utiliza seu conhecimento técnico avançado em informática para realização de ações positivas.

Em contrapartida, o cracker usa seu conhecimento técnico avançado em tecnologia para ações negativas como condutas criminosas ou ainda com a finalidade de prejudicar outrem.

No tocante a pichação de sites, Carneiro (2012, s.p.) denomina este tipo de sujeito como Defacers, os quais registram suas marcas ao invadir sites e desfiguram-as.

Os Defacers são sujeitos como se fora pichadores, entretanto suas atividades não são realizadas em muros e sim em sites, blogs e demais meios. (WENDT;JORGE, 2012, p.26)

Os Carders são sujeitos típicos estelionatários, umas vez que utilizam-se da obtenção de dados alheios, principalmente de dados de cartões de créditos, para a realização de compras. (CRESPO, 2011, p.96)

Estes sujeitos ainda podem atuar de forma a criar programas para a capturar dados de cartões e utilizá-los para compras, explorando a fragilidade do sistema de segurança da administradora de cartões de crédito ou ainda da negligência dos usuários na utilização dos seus respectivos cartões. (MEDEIROS, 2015, s.p.)

Os Lammers são os sujeitos os quais possuem um conhecimento não tão avançado quanto aos demais sujeitos dos crimes virtuais, mas que imaginam que detenham tal conhecimento. Em outras palavras, são novatos apenas deslumbrados que costumam acreditar que serem hackers. (CRESPO, 2011, p.97)

Para Neto (2005, p.267), os Lammers são iniciantes e “fazem o uso anti-social da rede, visando tão somente, a perturbar os demais usuários”.

Os Wannabes são os sujeitos que querem ser especialistas, mas que na verdade não são, uma vez que possuem pouco conhecimento e ainda não estão aptos para a prática de grandes crimes. (CRESPO, 2011, p.97)

Segundo Carneiro (2012, s.p.) os Wannabes “atuam em pequenos feitos limitando seus conhecimentos e não representam tanto perigo sendo classificados como leigos frente a grandes posições de hackers”.

A diferença entre Wannabes e Lammers é que aqueles possuem consciência de suas limitações o que os diferencia destes, (CRESPO, 2011, p.97)

Os Phreakers são sujeitos que são especialistas em telefonia, ou seja, usam de seus conhecimentos para que possam realizar ligações gratuitas e escutas, tudo por meio de computadores e dispositivos tecnológicos, desta forma confundem

as operadoras telefônicas de forma que estas identifiquem como um terceiro realizador de suas ligações. (CRESPO, 2011, p.97)

Sintetiza o conceito Carneiro (2012, s.p.) salientando que os Pheakers “cometem crimes específicos voltados para a área de telecomunicações”

Os White Hats e Black Hats, na tradução chapéu branco e chapéu preto, são sujeitos que podem ser identificados também como bons e maus hackers, pois praticam as invasões para o bem ou para o mau, neste caso delitivamente, respectivamente. (CRESPO, 2011, p.97)

Logo, define-se White Hats como o hacker do bem, pessoas de um vasto conhecimento mas que não o utiliza para a ilegalidade e muitas vezes agem para o bem, diferente dos White Blacks que são definidos como hacker do mal e usam de seus conhecimentos para ilícitos como roubo de senhas, documentos ou espionagem industrial. (LOURENÇO, 2013, p.16)

Por fim, o que pode-se concluir é que independente das características de cada conduta, há de se ter um conhecimento técnico avançado em tecnologia para que possa realizá-las. Isto torna estes sujeitos como ímpares, de características específicas.

5.2 SUJEITO PASSIVO

O sujeito passivo do crime pode ser definido como aquele que é titular do bem jurídico o qual é protegido por lei penal incriminadora e que tenha sido violado. (NUCCI, 2011, p.180)

Para Bitencout (2007, p.231) sujeito passivo “é o titular do bem jurídico atingido pela conduta criminosa”, podendo este ser o ser humano, o Estado, a coletividade ou ainda a pessoa jurídica.

Destarte, Ishida (2009, p.53) enfatiza que o sujeito passivo “pode ser geral (constante) que é o Estado e particular (eventual) que pode ser a pessoa física ou jurídica e ainda o próprio Estado ou a coletividade”.

No tocante a sujeito passivo em crimes virtuais, em comparação ao sujeito ativo desta mesma modalidade, é uma figura que se tem uma maior facilidade de descrever, uma vez que pode ser qualquer indivíduo que tenha um

bem jurídico tutelado lesado ou ameaçado de lesão por condutas realizados através de computador ou qualquer outro dispositivo tecnológico. (ORRIGO;FILGUEIRA, 2016, p.6)

O sujeito passivo nos crimes virtuais, de forma generalizada será sempre uma pessoa física ou uma pessoa jurídica qualquer, ou ainda uma entidade de natureza pública ou privada, que seja titular de um bem jurídico tutelado, ou seja, pode ser qualquer indivíduo, ainda que pessoa jurídica, que possa ter por exemplo: seus bens desviados, seu patrimônio deteriorado ou informações violadas. (CARNEIRO, 2012, s.p.)

Logo, qualquer pessoa física ou jurídica que tenha seu bem jurídico atingido por conduta realizada por meio de dispositivos tecnológicos podem ser sujeitos passivos de crimes virtuais.

6 PROCEDIMENTOS DOS CRIMES VIRTUAIS

No tocante aos procedimentos realizados nos crimes virtuais e abordados neste capítulo, dá-se destaque para a aplicação territorial para estes tipos de crimes, a jurisdição e competência acerca do tema e por fim a investigação e produção de provas.

6.1 APLICAÇÃO TERRITORIAL

O surgimento do mundo virtual apresenta novas concepções de tempo e espaço, gerando empecilhos a aplicação de leis tradicional e apresentando um novo entendimento a território, uma vez que rompem-se as barreiras de limites territoriais físicos.(CRESPO, 2011, p.117)

Com a internet e o ambiente virtual, não existem barreiras ou limites de separação física, pois a concepção de território passa a ser qualquer um dos pontos interligados a rede e que tenha acesso às informações. (FIORILLO;CONTE, 2016, p.203)

Destarte, o ambiente virtual além trazer benefícios, trouxe consigo também os antigos e novos malefícios, dentre estes a facilitação da prática de crimes já existentes e a possibilidade de criação de outros novos crimes. (CRESPO, 2011, p.117)

Os recursos tecnológicos passam a permitir inclusive que os criminosos ajam em parcerias organizadas, mesmo em locais diferentes, distantes e muitas vezes sem ao menos se conhecerem, para que possam cometer o crime. (WENDT;JORGE, 2012, p.181)

Pinheiro (2013, s.p.) salienta que a dificuldade em definir o espaço não é uma exclusividade da internet e sim uma generalidade contemporânea, haja vista o mundo globalizado:

> O problema não está apenas no âmbito da Internet, mas em toda sociedade globalizada e convergente, na qual muitas vezes não é possível determinar

> qual o território em que aconteceram as relações jurídicas, os fatos e seus efeitos, sendo difícil determinar que norma aplicar utilizando os parâmetros tradicionais. (PINHEIRO, 2013, s.p.)

Em que se pesem todas as dificuldades para a definição territorial, a lei penal brasileira, no tocante a sua aplicação, tem como regra a aplicação dentro de seu limite territorial, salvo os casos de tratados ou convenções internacionais nos quais também é permitido a aplicação de lei estrangeira, ou seja, a combinação destas aplicações dá origem a denominada territorialidade temperada. (FIORILLO;CONTE, 2016, p.207)

Conforme disciplina Jesus e Milagre (2016, s.p.) "no Brasil, a legislação que norteia a questão está relacionada nos arts. 5º, 6º e 7º do Código Penal".

Neste sentido, o artigo 5º do Código Penal Brasileiro disciplina que "Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional". (BRASIL, 1940, s.p.)

Com relação ao lugar do crime, a teoria aplicada aos crimes cometidos, determinando o local do crime, é a teoria da ubiquidade a qual apresenta a combinação de outras duas teorias, considerando uma ou outra, sejam elas a teoria da atividade que entende como local do crime o local da ação onde foi cometido e a teoria do resultado que prevê como local do crime o local aonde se deu o resultado da ação cometida. (CRESPO, 2011, p.117)

O Código Penal Brasileiro, apresenta a teoria da ubiquidade por meio de seu artigo 6º, através do qual considera-se local do crime, para fim de aplicação de leis, tanto o local do momento executivo quanto o local do momento consumativo do crime. (FIORILLO;CONTE, 2016, p.203)

Neste sentido, dispõe o referido artigo que "considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado". (BRASIL, 1940, s.p.)

Cabe ressaltar que nas palavras de Jesus (2008, p.127) "basta que a porção da conduta criminosa tenha ocorrido em nosso território para que ser aplicada a nossa lei", ou seja, para a aplicação da lei penal brasileira é imprescindível que o crime tenha tocado ao solo nacional.

O ambiente virtual não é um território propriamente, sendo assim, ganha importância o local da informação, pois é que este que indica minimamente o

lugar do crime. Ganha destaque neste caso crimes que são cometidos de forma parcial em diversos países. (CRESPO, 2011, p.117)

Neste diapasão, têm-se os crimes cometidos no exterior, neste caso diga-se crimes virtuais cometidos no exterior, o Código Penal Brasileiro, por meio de seu artigo 7º disciplina sobre a extraterritorialidade dispondo que ficam sujeitos à lei brasileira:

O inciso primeiro do artigo 7º do Código Penal Brasileiro prevê punição para aqueles cometerem crimes, neste caso inclusive crimes virtuais, contra o Presidente da República; patrimônio ou a fé pública da União; do Distrito Federal; Estado; Município; empresas públicas e sociedade de economia mista; autarquias e fundação; contra a administração pública e quem esteja a serviço destas; ou ainda em casos de genocídio quando o agente for brasileiro ou domiciliado em território nacional. (BRASIL, 1940, s.p.)

Já o inciso segundo prevê punição para os crimes cometidos previstos em tratados ou convenção e que o Brasil tenha compromisso de reprimir a conduta; crimes cometidos por brasileiros; ou ainda crimes que sejam cometidos em aeronaves ou embarcações brasileiras, mesmo que mercantes ou privados, e em território estrangeiro. (BRASIL, 1940, s.p.)

O parágrafo primeiro do artigo 7º do Código Penal Brasileiro disciplina que nos casos previstos no inciso primeiro, o agente é punido de acordo com as leis brasileiras, mesmo que tenha sido absolvido no estrangeiro. (BRASIL, 1940, s.p.)

Ainda no artigo 7º do Código Penal Brasileiro, o parágrafo segundo prevê uma dependência para aplicação de penas para as condutas realizadas no inciso segundo deste artigo, como a entrada do agente em território nacional; ser crime também no país em que o ato foi praticado; estar o crime incluído dentre aqueles que o ordenamento jurídico nacional prevê para extradição; o agente não ter sido absolvido ou cumprido a pena, no estrangeiro; não ter sido o agente perdoado no estrangeiro ou a punibilidade não esteja extinta, segundo a lei mais favorável. (BRASIL, 1940, s.p.)

Com relação ao crime cometido por estrangeiro contra brasileiro fora do Brasil, ainda que sejam crimes virtuais, o parágrafo terceiro do artigo 7º do Código Penal Brasileiro disciplina que:

> § 3º - A lei brasileira aplica-se também ao crime cometido por estrangeiro contra brasileiro fora do Brasil, se, reunidas as condições previstas no parágrafo anterior: a) não foi pedida ou foi negada a extradição; b) houve requisição do Ministro da Justiça. (BRASIL, 1940, s.p.)

Logo, neste caso aplica-se a lei brasileira para os casos de crimes virtuais cometidos por estrangeiros contra brasileiros, nos casos em que se reunidas às condições do parágrafo segundo do mesmo artigo: não foi pedida ou negada a extradição ou quando houver requisição do Ministro da Justiça.

A lei penal brasileira, no tocante a sua aplicação, tem como regra a aplicação dentro de seu limite territorial, porém, para casos de tratados ou convenções internacionais permite também a aplicação de lei estrangeira para os crimes praticados total ou parcialmente em território nacional, adotando ao princípio da territorialidade temperada. (JESUS, 2008, p.129)

Para Fiorillo e Conte (2016, p.321) “é inegável a necessidade de cooperação internacional entre os Estados, independente de qual será o responsável pela aplicação da legislação”.

No tocante a tratados e convenções, em 2001 na Hungria foi criada pelo Conselho da Europa a Convenção de Budapeste, também conhecida como Convenção sobre os Crimes Virtuais para que houvesse cooperação internacional entre os membros signatários para o combate a modalidade de crime. (WENDT;JORGE, 2012, p.182)

O Brasil não é signatário da Convenção de Budapeste, porém tende a se tornar, uma vez que sem a cooperação internacional, a dificuldade para esclarecer autoria deste tipo de crime aumenta consideravelmente. (WENDT;JORGE, 2012, p.182)

Por fim, o que pode-se concluir é que com o fator internet existente, a tarefa de definir o local do crime, bem como as leis que serão aplicadas é de extrema complexidade.

Nos casos ainda que envolvam agentes de outros países, mais difícil fica ainda a tarefa, uma vez que a autonomia do Brasil torna-se relativa e dependente de tratados ou convenções, bem como da colaboração dos signatários.

6.2 INVESTIGAÇÃO E PROVAS

Inicialmente cabe apurar e apresentar quem pode realizar a investigação criminal para os casos de crimes virtuais.

Conforme o artigo 144 da Constituição Federal, por meio de seu parágrafo 4º o qual aborda a responsabilidade de segurança pública pelo Estado, o qual indica como órgão responsável “às polícias civis, dirigidas por delegados de polícia de carreira, incumbem, ressalvada a competência da União, as funções de polícia judiciária e a apuração de infrações penais, exceto as militares”.

Entretanto, a súmula 234 do STJ atribui também o poder de investigação ao Ministério Público, discorrendo que “a participação de membro do Ministério Público na fase investigatória criminal não acarreta o seu impedimento ou suspeição para o oferecimento da denúncia”. (BRASIL, 2011, s.p.)

Logo, o poder para a investigação criminal para os crimes virtuais é dado a Polícia Civil e ao Ministério Público.

No tocante a investigação criminal nos casos de crimes virtuais, esta é de extrema complexidade e possui peculiaridades, como uma fase técnica inicialmente para que somente após seja realizada a investigação policial propriamente dita, ou seja, pode-se dizer que a investigação para estes casos é dividida em fase técnica e fase de campo. (WENDT;JORGE, 2012, p.52)

Na fase técnica da investigação de crimes virtuais são executadas e analisadas tarefas e informações com o objetivo de localizar o dispositivo tecnológico que foi utilizado para a ação criminosa. (WENDT;JORGE, 2012, p.52)

Um dos principais fatores para a investigação é tomar conhecimento da prática e identificar qual meio foi utilizado para a prática do crime. De acordo com o meio, as técnicas para apuração das informações são diferentes, principalmente no que tange a localização do dispositivo. (CAVALCANTE, 2013, s.p.)

Neste sentido, é possível elencar uma série de tarefas a serem realizadas na fase técnica para apurar as informações como: análise do relato da vítima com o intuito de preservar o material comprobatório e compreensão dos fatos; orientação a vítima para preservação do material comprobatório; coleta inicial de provas no ambiente virtual; registro de um boletim de ocorrências formalizando o fato; investigação inicial referente aos dados do autor; formalização de relatório ou

certidão das provas coletadas preliminarmente; representação perante ao Poder Judiciário para que se obtenha quebra de dados, conexão ou acesso e que se possa solicitar dados cadastrais para o provedores de conteúdo; e análise das informações prestadas pelos provedores de conteúdo. (WENDT;JORGE, 2012, p.52)

O objetivo da apuração das informações é a busca por evidências e neste caso evidências principalmente digitais, conforme conceitua Pinheiro (2013, s.p.), “evidência digital é toda informação ou assunto de criação ou intervenção humana ou não, que pode ser extraído de um compilado ou depositário eletrônico. E essa evidência deve estar em um formato de entendimento humano”.

São características das evidências dos crimes virtuais: a complexidade por se tratar de arquivos, fotos, dados digitalizados; da volatilidade, uma vez que pode-se apagar, alterar ou se perder facilmente as informações; a dificuldade no tratamento dos dados, visto que muitas vezes ficam juntos com uma grande quantidade de dados, dificultando a identificação. (MINISTÉRIO PÚBLICO FEDERAL - PROCURADORIA DA REPUBLICA NO ESTADO DE SÃO PAULO - GRUPO DE COMBATE AOS CRIMES CIBERNÉTICOS,s.d; s.p.)

Algumas informações são essenciais para que se chegue até o dispositivo tecnológico em que a conduta foi cometida, dentre elas os LOGS e o IP. (CAVALCANTE, 2013, s.p.)

Destarte, Pinheiro (2013, s.p.) enfatiza que “para se ter informações básicas e necessárias para coleta e guarda para os provedores de acesso, é necessário ter o registro de logs e os registros cadastrais dos usuários de IPs”.

Praticamente toda ação realizada na internet é de alguma forma registrada. Neste sentido, estas ações realizadas dão origem aos LOGS que são os registros gerados das ações do operador na internet e do caminho que as informações percorrem, não permitindo que haja um anonimato total na internet, pois cada página da internet acessada pelo usuário é registrada, sendo assim possível identificar o local onde houve o acesso e inúmeros outros dados. (CAVALCANTE, 2013, s.p.)

Para cada endereço que informamos para acesso ao site, há uma tradução para um número identificador do computador ao qual está se conectando. Este número é denominado como IP (Internet Protocol). (MINISTÉRIO PÚBLICO FEDERAL - PROCURADORIA DA REPUBLICA NO ESTADO DE SÃO PAULO - GRUPO DE COMBATE AOS CRIMES CIBERNÉTICOS,s.d; s.p.)

O número do IP é um número de protocolo na internet atribuído ao computador conectado a rede mundial de computadores, ou seja, é a identificação do computador que acessa ou do computador que é acessado na internet. (MINISTÉRIO PÚBLICO FEDERAL - PROCURADORIA DA REPUBLICA NO ESTADO DE SÃO PAULO - GRUPO DE COMBATE AOS CRIMES CIBERNÉTICOS,s.d; s.p.)

Há ainda outros três aspectos importantes a ressaltar no tocante a investigação que são as investigações envolvendo sites, e-mails e redes sociais.

Quando se trata de investigação a sites envolvidos a crimes, as informações principais, principalmente o detentor do domínio, o IP e os LOGS de operações realizadas no site, podem ser fornecidas pelo órgão gestor dos registros de domínios de cada país. (CAVALCANTE, 2013, s.p.)

No Brasil o órgão responsável é Registro.br, o qual disponibiliza por meio do endereço www.registro.br uma ferramenta para consulta da pessoa detentora do endereço do site, também denominado como domínio. Para consulta de domínios de sites de fora do Brasil o órgão a ser consultado é o IANA (Internet Assigned Numbers Authority), por meio da ferramenta disponibilizada através do endereço www.iana.org/domains/root/db. (CAVALCANTE, 2013, s.p.)

Em se tratando de crimes cometidos por e-mail a investigação não se baseia tão somente na mensagem e na sua preservação, mas também nas evidências encontradas no cabeçalho do e-mail, pois é neste local que estão localizadas informações importantes como remetente, destinatário, número de IP e data e hora transmissão da mensagem. A partir destas informações é que parte a investigação de local e autoria. (MINISTÉRIO PÚBLICO FEDERAL - PROCURADORIA DA REPUBLICA NO ESTADO DE SÃO PAULO - GRUPO DE COMBATE AOS CRIMES CIBERNÉTICOS,s.d; s.p.)

No caso das redes sociais, quando ocorrido fato criminoso no ambiente de alguma rede social, a investigação deverá solicitar, amparada por ordem judicial, a pessoa jurídica responsável por tal rede ou site para que forneça informações que possam levar ao autor, como logs de acesso, dados dos perfis de usuários e se necessário inclusive interceptação telemática do fluxo de dados. (CAVALCANTE, 2013, s.p.)

O Poder Judiciário pode ainda determinar ao administrador de rede de determinado local para que preste as informações técnicas específicas de forma que

possam auxiliar na identificação do local do dispositivo tecnológico ou do autor. Isto ocorre principalmente em rede corporativas, as quais devem obter as informações referentes aos acessos. (WENDT;JORGE, 2012, p.177)

Destarte, a guarda de dados de LOGS e IP's onde a lei 12965/2014, conhecida como "Marco Civil", disciplina sobre a responsabilidade da guarda dos dados de acesso pelo provedor de internet, principalmente em seu artigo 15º o qual dispõe que:

> Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento. (BRASIL, 2014, s.p.)

Identificado e localizado o dispositivo tecnológico que foi utilizado como meio para o crime, passa-se para a fase de campo na qual há o deslocamento de policiais e a realização das diligências com o objetivo de realizar o reconhecimento operacional de forma discreta, mas amparado pelo Poder Judiciário, principalmente no que toca ao mandado de busca e apreensão. (WENDT;JORGE, 2012, p.53)

Logo, cumpre concluir que as investigações dos crimes virtuais devem ser realizadas pelos entes competentes, utilizando de agentes que tenham o conhecimento técnico avançado e adequado para que se obtenha sucesso neste procedimento, o que possibilitará a geração de provas e indícios de forma segura e eficiente e consequentemente trará grandes possibilidades de encontrar a localização do dispositivo tecnológico, bem como do responsável pela conduta.

6.3 JURISDIÇÃO E COMPETÊNCIA

A jurisdição, segundo Nicolitt (2009, p.167) “é a função do Estado através do qual diz o direito no caso concreto”.

Em outras palavras, jurisdição é uma função do Estado, que representado pelo Poder Judiciário, aplica as normas da ordem em casos concretos de forma imparcial para a solução pacífica de litígios entre partes conflitantes, de forma a firmar a autoridade da ordem jurídica e a verticalidade na relação Estado-particular. (CAPEZ, 2015, p.257)

Entende-se por competência como a organização sistemática do exercício da jurisdição, ou seja, uma parcela da jurisdição que é entregue para cada órgão jurisdicional, fixando limites da atividade jurisdicional dentro do Poder Judiciário. (NICOLITT, 2009, p.168)

Logo, a competência segundo Capez (2015, p.259) “é a delimitação do poder de jurisdicional (fixa os limites dentro dos quais o juiz pode prestar jurisdição)”, sendo a fixação em razão de especialidades, sendo estas: de acordo com o a natureza do crime praticado, de acordo com a qualidade da pessoa incriminada ou ainda de acordo com o local que foi praticado o crime, local que foi consumado o crime ou o local da residência do autor. (CAPEZ, 2015, p.259)

O tema fica complexo a partir do momento que ocorre no ambiente virtual, ou seja, pela internet onde há extrema dificuldade na determinação territorial uma vez que o crime é cometido normalmente à distância, podendo ser inclusive pessoas de outros países e de outras culturas. (PINHEIRO, 2016, s.p.)

Isto posto, no tocante a fixação da competência, o artigo 70 do Código de Processo Penal Brasileiro determina como regra que “a competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução”. (BRASIL, 1941, s.p.)

Logo, tem-se como regra que os crimes serão julgados aonde foram consumados, ou seja, aonde o bem jurídico foi afetado. (ORRIGO;FILGUEIRA, 2016, p.6)

Nos casos de crimes virtuais que produzirem resultados em diversos locais dentro do território nacional, denominados plurilocais, ou ainda, no em casos

em que o crime ocorre em territórios não brasileiros, como crimes a distância ou de espaço máximo, a regulamentação é prevista por meio dos parágrafos do artigo 70 do Código Processual Penal Brasileiro.

O parágrafo primeiro do artigo 70 do Código de Processo Penal disciplina que “se, iniciada a execução no território nacional, a infração se consumar fora dele, a competência será determinada pelo lugar em que tiver sido praticado, no Brasil, o último ato de execução”.

Neste caso, fica fixada a competência, no caso do crime virtual ter iniciado em território nacional e consumado fora dele, como o lugar em tiver sido praticado o último ato em território nacional.

O parágrafo segundo do artigo 70 do Código de Processo Penal disciplina que “quando o último ato de execução for praticado fora do território nacional, será competente o juiz do lugar em que o crime, embora parcialmente, tenha produzido ou devia produzir seu resultado”.

Destarte, o parágrafo segundo prevê para os casos de crimes cometidos virtualmente, onde o último ato tenha ocorrido fora de território nacional, o juiz competente é o do lugar do crime em que produziu resultado, mesmo que parcialmente.

Por fim, o parágrafo terceiro do artigo 70 do Código de Processo Penal disciplina que “quando incerto o limite territorial entre duas ou mais jurisdições, ou quando incerta a jurisdição por ter sido a infração consumada ou tentada nas divisas de duas ou mais jurisdições, a competência firmar-se-á pela prevenção”.

Logo, quando o crime for consumado ou tentado em local incerto no que toca ao limite territorial entre duas ou mais jurisdições, firma-se a competência pela prevenção, ou seja, conforme previsto no artigo 83 do Código de Processo Penal, defini-se a competência quando concorrida por duas ou mais, para aquele que tiver antecedido aos outros. (BRASIL, 1941, s.p.)

O Tribunal de Justiça do Estado do Paraná também se pronuncia acerca da competência e a aplicação do artigo 70 do Código de processo Penal da seguinte forma:

> DECISÃO: ACORDAM os Magistrados integrantes da Segunda Câmara Criminal do Egrégio Tribunal de Justiça do Paraná, à unanimidade, em conhecer parcialmente do recurso, e, nessa parte, dar-lhe provimento. EMENTA: RECURSO EM SENTIDO ESTRITO. CRIMES CONTRA A HONRA PRATICADOS PELA INTERNET.ANÁLISE SOBRE A

> COMPETÊNCIA PARA APRECIAR A MATÉRIA. APLICAÇÃO DA REGRA DO ART. 70 DO CÓDIGO DE PROCESSO PENAL. TEORIA DO RESULTADO. LOCAL ONDE A VÍTIMA E TERCEIROS TOMARAM CONHECIMENTO DOS FATOS, EM TESE, OFENSIVOS, AINDA QUE AS PUBLICAÇÕES NO FACEBOOK TENHAM OCORRIDO EM LOCAL DIVERSO. RECURSO PARCIALMENTE CONHECIDO, E, NESSA PARTE, PROVIDO.Aplica-se a regra do art. 70 do Código de Processo Penal (lugar da consumação) nos crimes contra a honra, cometidos pela Internet (na rede social Facebook), tendo em vista que o conteúdo, em tese, ofensivo, pode ser publicado de qualquer lugar, contudo causam ofensas à honra da vítima na comunidade em que ela vive. I. (TJPR - 2ª C.Criminal - RSE - 1397104-5 - Região Metropolitana de Maringá - Foro Central de Maringá - Rel.: José Mauricio Pinto de Almeida - Unânime - - J. 08.10.2015) (TJ-PR - RSE: 13971045 PR 1397104-5 (Acórdão), Relator: José Mauricio Pinto de Almeida, Data de Julgamento: 08/10/2015, 2ª Câmara Criminal, Data de Publicação: DJ: 1678 28/10/2015)

Neste caso, o presente julgado deferiu parcialmente o recurso de sentido estrito sobre a competência para julgar a matéria, posicionando-se a favor definição da competência de acordo com o exposto no artigo 70 do Código de Processo Penal, ficando definida competente a jurisdição do local da consumação do crime.

O Código de Processo Penal Brasileiro ainda complementa a fixação da competência para os casos em que não se conhece o local do crime, disciplinando, por meio de seu artigo 72 que: “não sendo conhecido o lugar da infração, a competência regular-se-á pelo domicílio ou residência do réu”.

Cabe ressaltar ainda, com relação à definição de competência, o artigo 88 do Código de Processo Penal Brasileiro prevê que:

> Art 88.No processo por crimes praticados fora do território brasileiro, será competente o juízo da Capital do Estado onde houver por último residido o acusado. Se este nunca tiver residido no Brasil, será competente o juízo da Capital da República. (BRASIL, 1941, s.p.)

Os crimes virtuais trazem consigo algumas peculiaridades na fixação da competência por conta dos reflexos em diversos locais por conta da conduta do criminoso; da localização de servidores por todo o mundo, mas principalmente nos EUA, trafegando dados pela rede mundial; da hospedagem, ou seja, da localização física dos dados. (FIORILLO;CONTE, 2016, p.318)

Para estes casos, ainda não existe uma resposta definitiva, entretanto são adotados alguns critérios que auxiliam na definição da jurisdição, como: a proibição de jurisdição irrazoável, ou seja, uma jurisdição que não tenha relação com o ponto inicial ou final da comunicação e a desconsideração, em alguns casos, do

local da conexão a rede ou da hospedagem de dados para a determinação da jurisdição, cabendo análise ao caso concreto. (FIORILLO;CONTE, 2016, p.318)

No âmbito interno, a fixação da competência em crimes virtuais deve observar que a Internet resguardada dentro dos limites brasileiro é de interesse da União e que também há a possibilidade de envolvimento de elementos internacionais, sendo prudente a que a Justiça Federal seja competente. (VIANNA, 2000, p.19)

Destarte, o artigo 109 da Constituição Federal, em seus incisos IV e V disciplinam sobre a competência dos Juízes Federais para julgar os casos de

> IV- os crimes políticos e as infrações penais praticadas em detrimento de bens, serviços ou interesse da União ou de suas entidades autárquicas ou empresas públicas, excluídas as contravenções e ressalvada a competência da Justiça Militar e da Justiça Eleitoral. V - os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente; (BRASIL, 1988, s.p.)

Neste sentido, explica-se de acordo com o exposto no artigo 109, incisos IV e V, que os crimes virtuais serão da competência da Justiça Federal quando: se tratar de crimes contra políticos; bens ou serviços da União; entidades autárquicas ou empresas públicas; crimes previstos em tratado ou convenção internacional e por fim crimes contra o sistema financeiro ou à ordem econômico financeira, estes últimos nos casos previstos em lei. (FIORILLO;CONTE, 2016. p.329)

Posta a competência da Justiça Federal acerca dos crimes virtuais, fica competente, de forma residual a Justiça Estadual para julgar os demais crimes. (ORRIGO;FILGUEIRA, 2016, p.7)

Logo, a Justiça Estadual fica, em caráter residual, competente a processar e julgar crimes virtuais como por exemplo crime contra a honra de particular praticado por meio da internet. (FIORILLO;CONTE, 2016, p.329)

Pode-se concluir que, nas letras do ordenamento jurídico, bem como no entendimento dos doutrinadores, a Justiça Federal fica competente a julgar crimes contra agentes específicos e de forma residual, ou seja, com nos demais casos a competência é da Justiça Estadual.

7 CONCLUSÃO

O uso dos dispositivos tecnológicos passou a fazer parte do cotidiano da sociedade contemporânea, a que os doutrinadores chamam como sociedade da informação justamente por conta da forte influência da tecnologia e da velocidade de transmissão das informações na vida das pessoas.

Neste diapasão, dá-se destaque para a internet que contribuiu de forma importante para o mundo globalizado atual, mas principalmente influenciou nos costumes, dando novas formas tratar as atividades do dia-a-dia, disponibilizando informação a todo tempo e para o mundo todo, e estreitando os laços de comunicação entre as pessoas, de forma jamais imaginada e que ignora simplesmente distâncias de milhares de quilômetros.

Logo, o que se vê nos dias atuais são pessoas utilizando-se dia e noite das tecnologias e da internet em suas vidas para o benefício, ou seja, para realizar atividades profissionais e pessoais, comunicação, consumo, dentre outras atividades cotidianas.

Em contrapartida, apesar de trazer inúmeros benefícios à vida das pessoas, a tecnologia também trouxe uma nova preocupação para a sociedade.

Uma nova modalidade de crime estaria nascendo, fruto do glorificado avanço tecnológico. Nasciam os crimes virtuais, tema de extrema importância atualmente, tendo em vista a popularização das tecnologias e da internet, as que necessitam de ambiente seguro para que se tenha a normalidade social necessária.

Esta nova modalidade de crimes que são crimes realizados por meio algum dispositivo tecnológico para que se possa tingir algum bem jurídico de outrem.

Como tudo o que há de novo na sociedade deve se acompanhado de perto pelo Direito de forma que possa regular a vida social e punir sempre que necessário as condutas ilícitas e previstas no ordenamento jurídico, com os crimes virtuais não seria diferente.

Entretanto, no Brasil até o ano de 2012 ainda não havia nenhum tipo de lei específica para tipificar as condutas ilícitas realizadas por meio de computador ou dispositivo tecnológico. Em 2012 é criada a lei 12737/2012, denominada lei

Carolina Dieckmann, lei esta que daria enfase aos crimes cometidos por meio de dispositivo tecnológico.

Alteraram-se então alguns artigos do Código Penal Brasileiro.Porém, ainda que com lei específica criada, acreditou-se ainda que não seria o suficiente para regular a sociedade da informação no Brasil.

Neste sentido, surge o problema do presente trabalho que é apresentar como o Brasil abordou o tema crimes virtuais, no que toca a legislação penal, bem como as punições instituídas para as condutas e as características de cada um destes crimes.

Tão logo estipulado o problema, passou-se a apurar os aspectos relevantes aos crimes virtuais no Brasil em uma abordagem mais ampla, para que fossem pesquisadas especificamente cada uma das condutas perfunctoriamente e suas respectivas tipificações no ordenamento jurídico nacional, buscando desta forma dar uma visão do todo acerca do tema.

Destarte, abordou-se a tecnologia contemporânea e a sociedade contemporânea; o estudo dos crimes virtuais no Brasil no tocante a: legislação, sujeitos, local do crime, jurisdição e investigação para esta modalidade de crime.

No tocante a doutrina, apesar de ser um tema importante, foi encontrada certa dificuldade na pesquisa doutrinária, uma vez que ainda são poucos os doutrinadores que se manifestaram sobre o tema, talvez por ainda ser um tema recente e que exija a busca do conhecimento ou de pessoas especialistas em tecnologia para possam apoiá-los na emissão de algum ensinamento jurídico sobre o tema.

As hipóteses previstas eram a exposição no trabalho das leis e de doutrinas pesquisadas existentes acerca do tema, e a previsão de mais leis específicas sobre o tema, além das já existentes, de forma que pudessem complementar o ordenamento jurídico brasileiro no que toca a matéria de crimes virtuais.

Desta forma, passa-se a concluir o presente trabalho, baseado em todas as informações e dados levantados junto a doutrinas, leis e jurisprudência.

As hipóteses previstas no início do presente trabalho foram parcialmente positivas.

Atualmente não há dúvidas de que a tecnologia passou a fazer parte da vida das pessoas de forma permanente, haja vista a dependência das pessoas na realização de suas atividades.

O que se pode concluir acerca da legislação penal que toca aos crimes virtuais é de que hoje temos leis que podem punir a grande maioria das condutas realizadas por meio de computador, entretanto é importante que seja dada uma atenção maior e mais rápida ao tema.

Ainda percebe-se que algumas condutas específicas, como por exemplo o dano ao computador, ou seja, ao dispositivo tecnológico físico por meio de invasão virtual ou ainda o furto virtual por meio de invasão, não têm uma lei específica, utilizando-se das normas já existentes do Código Penal de 1940.

Logo, é importante que haja uma atualização para que sejam tratadas de acordo com o contexto moderno e da Sociedade Informação no Brasil.

Neste sentido, cabe ressaltar ainda a grande velocidade com que as tecnologias se desenvolvem, sendo missão complexa, porém importante ao direito, acompanhar a evolução tecnológica para que a sociedade não fique desamparada.

Quanto aos sujeitos desta modalidade de crime, os sujeitos ativos dos crimes virtuais são aqueles que possuem conhecimento técnico avançado em tecnologia, e que as os sujeitos que realizam as condutas desta modalidade de crime normalmente tem características e objetivos específicos, como hackers, crackers, dentre outros apresentados.

Já os sujeitos passivos, de forma geral são aqueles que têm bem jurídico atingido nos crimes virtuais, podendo ser pessoa física ou jurídica, de direito público ou privado.

Neste diapasão é importante que haja algum tipo de conscientização as mesmas, com instruções claras a respeito destas condutas e formas seguras de realizar suas atividades, de utilizar a internet e redes sociais.

Por fim, quanto aos procedimentos, pode-se concluir que no tocante a definição do local do crime, há certa complexidade acerca do tema e é necessário que se tenha de forma mais clara de definir estas situações.

Com relação a jurisdição competente, atualmente no Brasil é definida a competência à Justiça Federal a crimes virtuais, assim como demais crimes, contra entes específicos, e que residualmente compete a Justiça Estadual os demais casos.

Por fim, com relação a investigação e as provas no ambiente no virtual, conclui-se ainda que, apesar de todo o conhecimento tido hoje pelos profissionais da área e de todo o empenho das autoridades competentes, é necessário que haja investimento em novas tecnologias e em mão-de-obra qualificada por parte do Estado e entidades competentes para que possa acompanhar de igual para igual os criminosos especialistas em tecnologia e desta forma combater estes criminosos, inclusive de forma preventiva. Estes especialistas a cada dia ampliam seus conhecimentos tecnológicos, inclusive com informações do exterior local onde as novas tecnologias tendem a chegar primeiro.

REFERÊNCIAS

ALBERTIN, Alberto Luiz. **Comércio Eletrônico.** 3ª ed. São Paulo. Atlas, 2001.

ALBINO, Priscilla Linhares; TERÊNCIO, Marlos Gonçalves. **Considerações Críticas Sobre o Fenômeno do Bullying**: do Conceito ao Combate e à Prevenção. Ministério Público de Santa Catarina. Disponível em: <http://portal.mp.sc.gov.br/portal/conteudo/artigo%20bullying%20final.pdf>. Acesso em: 13 set. 2016.

ALENCAR, Marcio Aurelio dos Santos. **Fundamentos de Redes de Computadores.** Ministério da Educação e Cultura. Disponível em: <http://redeetec.mec.gov.br/images/stories/pdf/eixo_infor_ comun/tec_man_sup/081112_fund_redes_comp.pdf>. Acesso em: 20 Ago. 2016.

BECK, Leland L. **Desenvolvimento de Software básico.** Assemblers, linkers, loaders, compiladores, sistemas operacionais, banco de dados e processadores de textos. Tradução de Fernando Ximenes. Rio de Janeiro. Campus, 1993.

BENFICA, Alex. **O que é Smartphone?** Disponível em: <https://www.telefonescelulares.com.br/o-que-e-smartphone/>. Acesso em: 20 Ago. 2016.

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal.** 11ª ed. São Paulo. Saraiva, 2007.

BITTENCOURT, Thiago. **Entenda o que são vírus, spywares, trojans, worms e saiba como se proteger.** Disponível em: <http://www.techtudo.com.br/artigos/noticia/2013/06/entenda-o-que-sao-virus-spywares-trojans-worms-e-saiba-como-se-proteger.html> Acesso em: 04 Set. 2016.

BOZZA, Claudia. **Saiba o que é um navegador e um sistema operacional.** Disponível em: <http://www.techtudo.com.br/dicas-e-tutoriais/noticia/2011/08/saiba-o-que-e-um-navegador-e-um-sistema-operacional.html>. Acesso em: 20 Ago. 2016.

BRASIL. **Código Penal**. Decreto-lei nº 2848, de 7 dezembro de 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm>. Acesso em: 20 Ago. 2016.

BRASIL. **Código de Processo Penal**. Decreto-lei 3689, de 3 de outubro de 1941. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/Del3689.htm>. Acesso em: 20 Ago. 2016.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acesso em: 20 Ago. 2016.

BRASIL. Lei nº 8069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis /L8069Compilado.htm>. Acesso em: 27 Ago. 2016.

BRASIL. Lei nº 9279, de 14 de maio de 1996. Regula direitos e obrigações relativos à propriedade industrial. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9279.htm>. Acesso em: 15 Out. 2016.

BRASIL. Lei nº 10826, de 22 de dezembro de 2003. Dispõe sobre registro, posse e comercialização de armas de fogo e munição, sobre o Sistema Nacional de Armas – Sinarm, define crimes e dá outras providências. Disponível em <http://www.planalto.gov.br/ccivil_03/leis/2003/L10.826compilado.htm>. Acesso em: 15 Out. 2016

BRASIL. Lei nº 11343, de 23 de agosto de 2006. Institui o Sistema Nacional de Políticas Públicas sobre Drogas - Sisnad; prescreve medidas para prevenção do uso indevido, atenção e reinserção social de usuários e dependentes de drogas; estabelece normas para repressão à produção não autorizada e ao tráfico ilícito de drogas; define crimes e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11343.htm>. Acesso em: 15 Out. 2016.

BRASIL. Lei nº 11829, de 25 de novembro de 2008. 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. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/lei/l11829.htm>. Acesso em: 27 Ago. 2016

BRASIL. Lei nº 12737, 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: 27 Ago 2016.

BRASIL. Lei nº 12965, 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/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 17 Set. 2016.

BRASIL. Lei nº 13185, de 6 de novembro de 2015. Institui o Programa de Combate à Intimidação Sistemática (Bullying). Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2015/Lei/L13185.htm>. Acesso em: 27 Ago. 2016.

BRASIL. Superior Tribunal de Justiça. Habeas-Corpus. Tráfico. Pena-base. exasperação. legalidade. natureza e grande quantidade da droga apreendida. dedicação à atividade criminosa. Causa especial de diminuição. não incidência. Habeas Corpus: 176495/SP. Superior Tribunal de Justiça. Brasília, 21 de Junho de 2011. Disponível em: <http://www.stj.jus.br/SCON/jurisprudencia/doc.jsp?livre=%28%28%22MARIA+THEREZA+DE+ASSIS+MOURA%22%29.min.%29+E+%28%22Sexta+Turma%22%29.org.&data=%40DTDE+%3E%3D+20110621+e+%40DTDE+%3C%3D+20110621&b=ACOR&p=true&t=JURIDICO&l=10&i=23>. Acesso em: 15 Out. 2016.

BRASIL. Superior Tribunal Justiça. Súmula n.º 234. A participação de membro do Ministério Público na fase investigatória criminal não acarreta o seu impedimento ou suspeição para o oferecimento da denúncia.. Disponível em: <https://ww2.stj.jus.br/docs_internet/revista/eletronica/stj-revista-sumulas-2011_17_capSumula234.pdf>. Acesso em:15 Out. 2016.

BRASIL. Tribunal Regional Federal (4. Região). Habeas-Corpus. Condenação por furto qualificado. Habeas-Corpus n.º 50213979020144040000/SC, Tribunal Regional Federal – 4ª Região, Porto Alegre, RS, 16 de setembro de 2014. Disponível em: <http://www2.trf4.jus.br/trf4/controlador.php?acao=consulta_processual_resultado_pesquisa&txtValor=50213979020144040000&selOrigem=TRF&chkMostrarBaixados=&todaspartes=S&selForma=NU&todasfases=&hdnRefId=894ac43ecd86adb7c7965983a52c2541&txtPalavraGerada=WznN&txtChave=>. Acesso em: 15 Out. 2016

BRASIL. Tribunal Regional Federal (4. Região). Habeas-Corpus. Pedofilia. Habeas-Corpus n.º 41106/SC, Tribunal Regional Federal – 4ª Região, Porto Alegre, RS, 02 de dezembro de 2008. Disponível em: <http://www2.trf4.jus.br/trf4/controlador.php?acao=consulta_processual_resultado_pesquisa&txtValor=200872160006770&selOrigem=SC&chkMostrarBaixados=&todaspartes=S&selForma=NU&todasfases=&hdnRefId=&txtPalavraGerada=&txtChave=>. Acesso em: 15 Out. 2016

CABETTE, Eduardo Luiz Santos. **Lei Carolina Dieckmann**: O novo crime de Invasão de Dispositivo Informático. Disponível em: <http://www.conjur.com.br/2013-fev-04/eduardo-cabette-crime-invasao-dispositivo-informatico>. Acesso em: 04 Set. 2016.

CAPEZ, Fernando. **Curso de Direito Penal.** Parte Geral. Volume 1. 8ª ed. São Paulo. Saraiva, 2005.

_____. **Curso de Direito Penal.** Legislação Penal Especial. Volume 4. 9ª ed. São Paulo. Saraiva, 2014.

_____, **Curso de Processo Penal.** 22ª ed. São Paulo. Saraiva, 2015.

CASADO, Aline Gabriela Pescaroli. **Cyber bullying**: violência virtual e o enquadramento penal no Brasil. Revista Jurídica Eletrônica Âmbito Jurídico. Rio Grande do Sul, XIV, n. 95, 2011. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=10882>. Acesso em: 15 out. 2016.

CENTRO DE ESTUDOS, RESPOTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Cartilha de Segurança para Internet**. Disponível em: <http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 10 Set. 2016.

CAPRON, H.L. JOHNSON J.A. **Introdução a Informática.** Tradução de José Carlos Barbosa dos Santos. São Paulo. Pearson Prentice Hall, 2004.

CARDOSO, Mayara. **Evolução dos Computadores.** Disponível em: <http://www.infoescola.com/informatica/evolucao-dos-computadores>. Acesso em: 25 Abr 2016.

CARNEIRO, Adaneele Garcia. **Crimes virtuais: Elementos para uma reflexão sobre o problema na tipificação.** Revista Jurídica Eletrônica Âmbito Jurídico. Rio Grande do Sul, XV, n.99, 2012. Disponível em: <http://www.ambito- juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_id=11529>. Acesso em: 27 Ago 2016.

CAVALCANTE, Waldek Fachinelli. **Provas Processuais Penais:** Interceptação telefônica e telemática na legislação brasileira e jurisprudência atual do Supremo Tribunal Federal. Disponível em: <https://jus.com.br/artigos/30444/provas-processuais-penais>. Acesso em: 13 Set. 2016

_____, **Crimes cibernéticos**: noções básicas de investigação e ameaças na internet. Disponível em: <https://jus.com.br/artigos/25743/crimes-ciberneticos>. Acesso em: 22 Out. 2016.

CHAGAS, Ariana et al. **O Conceito de Tecnologia:** Pressupostos de Valores Culturais Refletidos nas Práticas Educacionais. Disponível em: <http://www.pucpr.br/eventos/educere/educere2008/anais/pdf/460_449.pdf>. Acesso em: 21 Abr 2016.

COELHO, Fabio Ulhoa. **Manual de Direito Comercial.** 25ª ed. São Paulo. Saraiva, 2013.

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

FACULDADES INTEGRADAS SANTA CRUZ DE CURITIBA. **Normalização de apresentação de trabalhos científicos do curso de Direito**, Curitiba, 2015. 53 p. Disponível em: < http://www.santacruz.br/v4/download/manual-de-normalizacao-do-curso-de-direito.pdf>. Acesso em: 03 set. 2015.

FOROUZAN, Behrouz A. **Comunicação de Dados e Redes de Computadores**. Tradução de Ariovaldo Griesi. 4 ed. São Paulo. McGraw-Hill, 2008.

GATTO, Victor Henrique Gouveia. **Tipicidade penal dos crimes cometidos na internet**. Revista Jurídica Eletrônica Âmbito Jurídico. Rio Grande do Sul, XIV, n. 91, ago 2011. Disponível em: <http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_ id=9962&revista_caderno=17>. Acesso em: 15 Out. 2016.

GRECO, Rogerio. **Comentários sobre o crime de invasão de dispositivo informático Art. 154-A do Código Penal.** Disponível em: < http://www.rogeriogreco.com.br/?p=2183>. Acesso em: 09 Set. 2016.

GIL, Antonio Carlos. **Como Elaborar Projetos de Pesquisa.** 4ª ed. São Paulo: Atlas, 2002. 61 p.

GUIMARÂES, Deocleciano Torrieri. **Dicionário Compacto Jurídico.** 16ª ed. São Paulo. Rideel, 2012.

IANA – INTERNET ASSIGNED NUMBERS AUTHORITY. Disponível em: <http://www.iana.org/domains/root/db>. Acesso em: 22 Out. 2016.
IESDE – INTELIGÊNCIA EDUCACIONAL E SISTEMAS DE ENSINO. **Curso de informática básica.** Disponível em <http://uol.iesde.com.br/aprovaconcursos/demo_aprova_concursos /informatica_07.pdf>. Acesso em: 25 Abr. 2016.

JESUS, Damasio E. de. **Direito Penal.** 29ª ed. São Paulo. Saraiva, 2008.

JESUS, Damasio de; MILAGRE, José Antonio. **Manual de Crimes Informáticos.** São Paulo. Saraiva, 2016.

KOZAK, Dalton Vinicius. **Conceitos Básicos de Informática.** Disponível em: <https://chasqueweb.ufrgs.br/~paul.fisher/apostilas/inform/Conceitos.Basicos.da.Informatica.PDF>. Acesso em: 12 Mar. 2015.

KUROSE, James F. ROSS, Keith W. **Redes de Computadores e a Internet: uma nova abordagem.** Tradução de Arlete Simille Marques. 1ª ed São Paulo. Addison Wesley, 2003.

LOURENÇO, Tiago José Bandeira. **Vulnerabilidades em Redes Windows**. 2013. Campina Grande. 2013. 46f. Trabalho acadêmico – (Licenciatura da Computação) – Curso de Licenciatura da Computação, Universidade Estadual da Paraíba, Campina Grande, 2013. Disponível em:

<http://dspace.bc.uepb.edu.br/jspui/bitstream/123456789/2349/1/PDF%20-%20Tiago%20Jos%C3%A9%20Bandeira%20Louren%C3%A7o.pdf>. Acesso em 02 Nov. 2016.

MARÇULA, Marcelo. FILHO, Pio Armando Benini. **Informática: Conceitos e Aplicações.** 3ª ed. São Paulo. Érica, 2008.

MEDEIROS, Diego. **Crimes Virtuais.** Disponível em: <https://jus.com.br/artigos/42734/crimes-virtuais>. Acesso em: 15 Out. 2016.

MILAGRE, José Antonio. **A criminalização do Spam no Brasil. O que muda no marketing?**, Disponível em: <https://www.ecommercebrasil.com.br/eblog/2013/10/03/criminalizacao-spam-brasil-muda-marketing/>. Acesso em: 08 Out. 2016.

MINISTÉRIO PUBLICO DO DISTRITO FEDERAL E TERRITÓRIOS. **Injúria Racial x Racismo.** Disponível em: <http://www.mpdft.mp.br/portal/index.php/conhecampdft-menu/nucleos-menu/ncleo-de-enfrentamento-discriminao-ned-mainmenu-130/3047-injuria-racial-x-racismo>. Acesso em: 09 Set. 2016.

MINISTÉRIO PÚBLICO FEDERAL - PROCURADORIA DA REPUBLICA NO ESTADO DE SÃO PAULO - GRUPO DE COMBATE AOS CRIMES CIBERNÉTICOS. **Crimes Cibernéticos.** Manual Prático de Investigação. Disponível em: <https://www2.mppa.mp.br/sistemas/gcsubsites/upload/60/ManuaL%20Pr%C3%83%C2%A1tico%20de%20Investiga%C3%83%C2%A7%C3%83%C2%A3o%20sobre%20Crimes%20de%20Inform%C3%83%C2%A1tica.PDF>. Acesso em 15 Out 2016.

NASCIMENTO, Luciano Ricardo. **O direito penal econômico brasileiro e os crimes de concorrência desleal na era da globalização.** Revista Espaço Acadêmico. Paraná. Nº 136, set 2012. Disponível em: <http://eduem.uem.br/ojs/index.php/EspacoAcademico /article/viewFile/16015/9736>. Acesso em: 15 Out. 2016.

NETO, Nelson Burin. **A Parte Especial do Código Penal Brasileiro Frente a Criminalidade na Informática**. Revista do Instituto de Pesquisas e Estudos – Divisão Jurídica da Faculdade de Direito de Bauru, nº 44, p.263-280, set a dez de 2005. Disponível em: <https://www.ite.edu.br/ ripe_arquivos/ripe44.pdf#page=263>. Acesso em: 25 Abr. 2016.

NICOLITT, André. **Manual de Processo Penal.** Rio de Janeiro. Elsevier, 2009.

NUCCI, Guilherme de Souza. **Manual do Direito Penal.** 7ª ed. São Paulo. Revista dos Tribunais, 2011.

OLIVEIRA, Luiz Gustavo Caratti de; DANI, Marília Gabriela Silva. **Os crimes virtuais e a impunidade real**. Revista Jurídica Eletrônica Âmbito Jurídico, Rio Grande do Sul, XIV, n. 91, ago 2011. Disponível em: <http://www.ambito-juridico.com.br/site/?n_link=revista_ artigos_leitura&artigo_id=9963&revista_caderno=17>. Acesso em 15 Out. 2016.

NUCLEO DE COMBATE AOS CIBERCRIMES – NUCIBER. Disponível em: <http://www.nuciber.pr.gov.br/>. Acesso em: 15 Out. 2016.

OLIVEIRA, Rodolpho Silva. **A sociedade da informação: princípios e relações jurídicas**. Revista Jurídica Eletrônica Âmbito Jurídico, Rio Grande do Sul, XIV, n. 95, dez 2011. Disponível em: <http://www.ambito-juridico.com.br/site/?n_link=revista_artigos_leitura&artigo_ id=10792&revista_caderno=17>. Acesso em: 25 Abr. 2016.

ORRICO, Alexandre; TUROLLO JUNIOR, Reynaldo; PAGNAN, Rogério. **Na internet 'secreta', droga proibida é vendida por R$ 1**. Jornal Folha de São Paulo On-line. Out. 2014. Disponível em: <http://www1.folha.uol.com.br/cotidiano/2014/10/1538399-na-internet-secreta-droga-proibida-e-vendida-por-r-1.shtml>. Acesso em: 27 Ago. 2016.

ORRIGO, Gabriel Marcos Archanjo; FILGUEIRA, Matheus Henrique Balego. **Crimes Cibernéticos:** Uma abordagem jurídica sobre os crimes realizados no âmbito virtual. Disponível em: < http://www.egov.ufsc.br/portal/conteudo/crimes-cibern%C3%A9ticos-uma-abordagem-jur%C3%ADdica-sobre-os-crimes-realizados-no-%C3%A2mbito-virtual>. Acesso em: 15 Out. 2016

O'REILLY, Tim. MILSTEN, Sarah. **Desvendando o Twitter.** Tradução de Eduardo Fraguas e Mariana Ribeiro. São Paulo. Universo dos Livros, 2009.

PAIVA, Raphael Rosa Nunes Vieira de. **Crimes Virtuais.** 2012. 55f. Trabalho acadêmico – (Graduação em Direito) – Curso de Direito, Centro Universitário do Distrito Federal, Brasília, 2012. Disponível em: <http://www.conteudojuridico.com.br/pdf/cj037145.pdf>. Acesso em: 25 Abr. 2016.

PARANÁ. Tribunal de Justiça do Estado do Paraná. Recurso em Sentido Estrito. Crimes contra a honra praticados pela internet. Análise sobre a competência para apreciar a matéria. aplicação da regra do art. 70 do código de processo penal. Teoria do resultado. Local onde a vítima e terceiros tomaram conhecimento dos fatos, em tese, ofensivos, ainda que as publicações no facebook tenham ocorrido em local diverso. Recurso parcialmente conhecido, e, nessa parte, provido. Relator: José Mauricio Pinto de Almeida. Jaguariaíva, 08 de outubro de 2015. Disponível em: <http://portal.tjpr.jus.br/jurisprudencia/j/12024261/Ac%C3%B3rd%C3%A3o-1397104-5>. Acesso em: 15 Out. 2016.

PARANÁ. Tribunal de Justiça do Estado do Paraná. Recurso em Sentido Estrito. Crimes contra a honra praticados pela internet (Facebook). Queixa-crime recebida apenas pelo crime de injuria. Pleito de recebimento pelos crimes de calunia e difamação. Calunia não caracterizada. Fatos que se referem a terceira pessoa e não ao querelante. Afastamento. Difamação. Ofensa à honra objetiva (reputação) do querelante. Conduta que não configura bis in idem com o crime de injúria. Bens jurídicos distintos. Recurso parcialmente provido. Relator: José Mauricio Pinto de Almeida. Maringá, 25 de fevereiro de 2016. Disponível em: <http://portal.tjpr.jus.br/jurisprudencia/j/12112703 /Ac%C3%B3rd%C3%A3o-1462862-5>. Acesso em: 15 Out. 2016.

PINTO, Márcia Rossana Oliveira. **Redação:** E-mail e Carta Comercial**.** Disponível em: <http://ftp.comprasnet.se.gov.br/sead/licitacoes/Pregoes2011/PE091/Anexos/Co mercio_modulo_I/etec%20reda%E7ao/redacao_08.pdf>. Acesso em: 20 Ago. 2016.
PICON, Rodrigo. **Diferença entre falsidade ideológica e falsa identidade.** Disponível em: <https://jus.com.br/artigos/38663/diferenca-entre-falsidade-ideologica-e-falsa-identidade. Acesso em: 17 Set. 2016.

PORTAL EDUCAÇÃO. **História da Informática.** Disponível em: <http://www.portaleducacao.com.br/informatica/artigos/53792/historia-da-informatica#ixzz46z9x1lbX>. Acesso em 25 Abr. 2016.

PRESSMAN, Roger S. **Engenharia de Software.** Tradução de José Carlos Barbosa dos Santos São Paulo. Makron Books, 1995.

REGISTRO.BR. Disponível em: <www.registro.br>. Acesso em 22 Out. 2016.

REIS, Júnias Belmont Alves dos. **O Conceito de Tecnologia e Tecnologia Educacional para Alunos do Ensino Médio e Superior**. In: ANAIS DO CONGRESSO DE LEITURA DO BRASIL DA ASSOCIAÇÃO DE LEITURA DO BRASIL. Campinas, 2009. Disponível em <http://alb.com.br/arquivo-morto/edicoes_anteriores/anais17/txtcompletos/sem16/COLE_932.pdf>. Acesso em: 19 Abr. 2016.

RIBEIRO, Felipe Oscar. **Crimes Virtuais:** Aspectos Atuais e Relevantes**.** 2013. Curitiba: 2013. 77f. Trabalho acadêmico – (Graduação em Direito) – Curso de Direito, Faculdades Integradas Santa Cruz, Curitiba, 2013.

RIO GRANDE DO SUL. Tribunal de Justiça Alçada Criminal. Apelação. Funcionário Público da CEEE. Essência dos crimes de alteração de sistema informatizado - circunstâncias judiciais favoráveis – pena base fixada no mínimo – Crime cibernético tipificado no art. 313-A do Código Penal. ACR: 70043570068 -RS.Agravantes: Espiral Filmes Ltda e outro. Agravado: Banco Banorte S. A. Relator: Luis Carlos de Barros. Pelotas, 06 de novembro de 2011. Disponível em: <http://www.tjrs.jus.br/busca/search?q=70043570068&proxystylesheet=tjrs_index&client=tjrs_index&filter=0&getfields=*&aba=juris&entsp=a__politica-site&wc=200&wc_mc=1&oe=UTF-8&ie=UTF-8&ud=1&lr=lang_pt&sort=date%3AD%3AR%3Ad1&as_qj=&site=ementario&as_epq=&as_oq=&as_eq=&as_q=+#main_res_juris>. Acesso em: 15 Out. 2016.

SADLER, Will. **Usando E-mail na Internet**. Rio de Janeiro. Campus, 1996.

SANTOS, Coriolano Aurélio de Almeida Camargo. **As múltiplas faces dos Crimes Eletrônicos e dos Fenômenos Tecnológicos e seus reflexos no universo Jurídico.** São Paulo. OAB-SP, 2009. Disponível em: <http://pt.scribd.com/doc/24156044/I-Livro-sobre-Crimes-Eletronicos-da-OAB-SP>. Acesso em: 27 Ago. 2016.

SILVA, Everton Augusto da. **O Uso de Dispositivos Tecnológicos na Educação:** concepções dos licenciandos para a prática pedagógica. 2015. 107f. Dissertação (Mestrado em Educação) – Universidade do Vale do Sapucaí, Pouso Alegre, 2015. Disponível em: <http://www.univas.edu.br/me/docs/dissertacoes2/37.pdf>. Acesso em: 22 Out 2016.

SILVEIRA, Artur Barbosa da. **Os crimes cibernéticos e a Lei nº 12.737/2012**. Disponível em: <http://www.conteudojuridico.com.br/artigo,os-crimes-ciberneticos-e-a-lei-no-127372012,52253.html>. Acesso em: 08 Out. 2016.

SILVEIRA, Rosimari Monteiro Castilho Foggiatto; BAZZO, Walter Antonio. Ciência e **Tecnologia:** Transformando a relação do ser humano com o mundo. IX SIMPÓSIO INTERNACIONAL PROCESSO CIVILIZADOR. Ponta Grossa, 2005. Disponível em: <http://www.uel.br/grupo-estudo/processoscivilizadores/portugues/sitesanais/anais9/artigos/workshop/art19.pdf>. Acesso em: 21 Abr 2016.

TAURION, Cezar. **Internet Móvel:** Tecnologias, Aplicações e Modelos. Rio de Janeiro. Campus, 2002.

TANENBAUM, Andrew S. **Redes de Computadores.** Tradução Vandenberg D. de Souza. 4ª ed. Rio de Janeiro. Elsevier, 2003.

TELLES, Andre. **Orkut.com**. São Paulo. Landscape, 2006.

VERASZTO, Estéfano Vizconde et al. **Tecnologia:** buscando uma definição para o conceito. Revista de Ciências e Tecnologias de Informação e Comunicação do CETAC.MEDIA. Campinas, n. 08, 2009. Disponível em: <http://revistas.ua.pt/index.php/prismacom/article/view/690/pdf>. Acesso em: 19 Abr 2016.

VIANA, Mateus Mosca. **Fundamentos da Informática para Universitários.** Rio de Janeiro: Brasport, 1996.

VIANNA, Tulio Lima. **Do delito de dano e de sua aplicação ao Direito Penal informático.** Disponível em: <https://jus.com.br/artigos/5828/do-delito-de-dano-e-de-sua-aplicacao-ao-direito-penal-informatico>. Acesso em: 04 Set 2016.

VIEIRA, Anderson da Silva. **Twitter –** Influenciando Pessoas e Conquistando o Mercado. Rio de Janeiro. Alta Books, 2009.

WERTHEIN, Jorge. **A sociedade da informação e seus desafios.** Disponível em: <http://www.scielo.br/pdf/ci/v29n2/a09v29n2.pdf>. Acesso em: 22 Out 2016.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos.** Ameaças e Procedimentos de Investigação. Rio de Janeiro. Brasport, 2012.

WILLRICH, Roberto. **Conceitos Básicos de Informática**. Disponível em: <http://professores.dcc.ufla.br/~monserrat/icc/Historia2.pdf>. Acesso em: 22 Abr 2016.

ZANELLATO, Marco Antonio. **Condutas Ilícitas na Sociedade Digital.** Direito e Internet. Caderno Jurídico da Escola do Ministério Público de São Paulo. São Paulo, Ano 2, Vol 1, nº 4, p.165-228, Jul 2002. Disponível em <http://www.mpsp.mp.br/portal/page/portal/Escola_Superior/Biblioteca/Cadernos_Tematicos/direito_e_internet.pdf>. Acesso em: 25 Abr. 2016.