AJES – FACULDADE DE CIÊNCIAS CONTÁBEIS E ADMINISTRAÇÃO DO VALE DO JURUENA
CURSO: BACHARELADO EM DIREITO

CRIMES INFORMÁTICOS: ANÁLISE DE SEUS ASPECTOS E AS DIFICULDADES DE REPRESSÃO DOS CRIMES

Autor: Alexandre Iwao Kubota
Orientador: Prof. Me. Caio Fernando Gianini Leite

JUÍNA/2016

AJES – FACULDADE DE CIÊNCIAS CONTÁBEIS E ADMINISTRAÇÃO DO VALE DO JURUENA

CURSO: BACHARELADO EM DIREITO

CRIMES INFORMÁTICOS: ANÁLISE DE SEUS ASPECTOS E AS DIFICULDADES DE REPRESSÃO DOS CRIMES

Autor: Alexandre Iwao Kubota

Orientador: Prof. Me. Caio Fernando Gianini Leite

Trabalho apresentado como exigência parcial para a obtenção do título de Bacharel em Direito, da Faculdade de Ciências Contábeis e Administração do Vale do Juruena – AJES.

JUÍNA/2016

AJES – FACULDADE DE CIÊNCIAS CONTÁBEIS E ADMINISTRAÇÃO DO VALE DO JURUENA

BANCA EXAMINADORA

_____

Prof. Me. Severino Erasmo de Lima

_____

Prof. Me. José Natanael Ferreira

_____

Orientador Prof. Me. Caio Fernando Gianini Leite

Dedico este trabalho a minha família, por sua capacidade de acreditar e me incentivar. Mãe, seu cuidado e dedicação foi que deram, em todos os momentos, a esperança para seguir. Pai, sua presença significou segurança e certeza de que não estou sozinho nessa caminhada.

AGRADECIMENTOS

A Deus por ter me dado saúde e força para superar as dificuldades.

Aos meus pais, pelo amor, incentivo e apoio incondicional.

A Faculdade, seu corpo docente, direção e administração que abriram a porta que hoje vislumbro um horizonte superior.

Ao meu orientador Caio Fernando Gianini Leite, pelo suporte, confiança, correções e incentivos.

E a todos que direta ou indiretamente fizeram parte da minha formação, em especial meus amigos Marcelo Faresin, Ranmar Santyago e Higor Dantas.

RESUMO

O foco deste trabalho está na análise dos aspectos dos crimes informáticos, tratando de conceitos, classificações e características, bem como no quão difícil é reprimir essa modalidade criminosa. Com efeito, o objetivo principal do trabalho é demonstrar que a legislação brasileira não é capaz de combater os crimes informáticos, assim como o aparato investigativo, que carece de incentivo e programas de especialização no tema, bem como a impossibilidade de fixação de competência jurisdicional para apurar e julgar os crimes. No decorrer do trabalho serão analisadas leis nacionais e a Convenção de Budapeste, a qual o Brasil não é signatária, a fim de demonstrar que a lei interna possui lacunas e muitas condutas tratadas na Convenção não está incorporada no ordenamento jurídico brasileiro. Ao final, aponta, em sede de conclusão, a necessidade de relativização da noção de soberania, para consecução de instrumentos jurídicos de cooperação internacional em matéria criminal, que fomentem a atuação conjunta dos países no tocante a harmonização das leis, a investigação policial e delimitação de competências.

Palavra-chave: Direito Penal – Crimes Informáticos – Internet – Dificuldade na repreensão do crime.

ABSTRACT

The focus of this work is on the analysis of aspects of computer crimes, dealing with concepts, classifications and characteristics, as well as how difficult it is to suppress this criminal modality. In fact, the main objective of the work is to demonstrate that Brazilian legislation is not capable of combating computer crimes, as well as the investigative apparatus, which lacks incentive and specialized programs in the subject, as well as the impossibility of establishing jurisdictional competence for Investigate and prosecute crimes. In the course of the work, national laws will be analyzed, and the Budapest Convention, to which Brazil is not a signatory, in order to demonstrate that the domestic law has gaps and many of the acts dealt with in the Convention are not incorporated into the Brazilian legal system. At the end, it points out, in conclusion, the need to relativize the notion of sovereignty, in order to achieve legal instruments of international cooperation in criminal matters, that foster the joint action of the countries with regard to harmonization of laws, police investigation and demarcation of skills.

Keyword: Criminal Law - Computer Crimes - Internet - Difficulty in crime repression.

SUMÁRIO

1 INTRODUÇÃO 8
2 O DESENVOLVIMENTO DA TECNOLOGIA NA SOCIEDADE 10
2.1 HISTÓRIA DO COMPUTADOR 12
2.2 HISTÓRIA DA INTERNET 14
2.3 A INTERNET NO BRASIL 19
2.4 DIREITO E A INFORMATIZAÇÃO 20
3 CRIMES INFORMÁTICOS 25
3.1 CONCEITO 25
3.2 BEM JURÍDICO 29
3.3 CLASSIFICAÇÃO 30
3.4 SUJEITOS DO CRIME 33
3.4.1 SUJEITO ATIVO 33
3.4.2 SUJEITO PASSIVO 35
3.5 DELITOS INFORMÁTICOS EM ESPÉCIE 36
3.5.1 CRIMES CONTRA A PESSOA 36
3.5.2 DOS CRIMES CONTRA O PATRIMÔNIO 48
4 INOVAÇÕES LEGISLATIVAS: O ADVENTO DA TUTELA DOS CRIMES INFORMÁTICOS E AS DIFICULDADES NA REPRESSÃO DOS CRIMES 54
4.1 CONVENÇÃO DE BUDAPESTE 54
4.2 LEI CAROLINA DIECKMANN (LEI Nº. 12.737/2012) 61
4.3 MARCO CIVIL DA INTERNET (LEI Nº. 12.965/2014) 67
4.4 A INCAPACIDADE PROFISSIONAL E TÉCNICA DOS ÓRGÃOS DE INVESTIGAÇÃO 73
4.5 O PROBLEMA DA COMPETÊNCIA 75
5 CONSIDERAÇÕES FINAIS 79
REFERÊNCIAS BIBLIOGRÁFICAS 81

1 INTRODUÇÃO

Com o surgimento das novas tecnologias, especialmente a internet, a sociedade passou por mudanças relevantes, as quais impulsionaram o processo de globalização. O advento da informática provocou mudanças culturais, tornando-a indispensável no dia a dia, tendo em vista que a maior parte das atividades é realizada através da internet.

O presente trabalho aborda a relação existente entre o Direito Penal e a informática, demonstrando que o ordenamento jurídico precisa evoluir consideravelmente para acompanhar a nova realizada social. O Direito Penal ainda não se adaptou ao novo contexto, principalmente porque o avanço tecnológico e informático é frenético.

Com efeito, assim como trouxe mudanças significativa na vida das pessoas, a internet trouxe consigo o indesejado aumento da criminalidade, tendo em vista que está sendo utilizada para a prática de condutas criminosas. A internet possibilitou a criação de novos crimes, que violam bens jurídicos no mundo todo.

Conforme se verificará no decorrer desse trabalho, a legislação penal brasileira precisa se atualizar para que possa reprimir as condutas praticadas no âmbito da internet.

Destaca-se, outrossim, que essa nova modalidade criminosa, conhecida como criminalidade informática, atinge diversos países, inclusive de maneira simultânea. Esse caráter transnacional dos crimes informáticos ensejará um grande problema mundial, qual seja, a dificuldade de fixar a competência jurisdicional, isto é, como o crime é praticado em vários países ao mesmo tempo, que país terá competência para apurar e julgar o crime? Ao longo desse trabalho será possível verificar que essa questão ainda não possui resposta.

Ademais, será observado que o problema da criminalidade informática também reside no âmbito investigativo, ante a ausência de profissionais capacitados para investigar os crimes.

Por fim, será possível concluir que a resolução dos problemas se dará com o cooperativismo internacional, pois os países precisam, em conjunto, estudar medidas,

tipificar crimes, estabelecer penas e definir competências, de modo que o criminoso não seja beneficiado com a lacuna legal e volte a transgredir.

2 O DESENVOLVIMENTO DA TECNOLOGIA NA SOCIEDADE

A necessidade de obter conhecimento; a busca pela informação, é o pilar da existência do homem. O aperfeiçoamento dos meios de produção e distribuição (a industrialização) derivam do aprendizado, cuja informação também é utilizada para melhorar a qualidade de vida das pessoas.

> A história da humanidade é habitualmente descrita em termos de eras cujos nomes refletem as etapas de desenvolvimento pelas quais ela passou: a idade da pedra, a idade do bronze, a idade do ferro e assim por diante, de modo a chegar até a era industrial, que estabeleceu os fundamentos de nossa sociedade industrial moderna. Hoje em dia é cada vez mais admitido em geral que ingressamos em uma nova era, uma etapa pós-industrial, em que a capacidade de utilizar a informação se tornou decisiva, não apenas para a produção dos bens, mas também para os esforços que procuram melhorar a qualidade de vida. Essa nova era é cada vez mais denominada por todos de era da informação.[1]

No decorrer dos séculos o acesso à informação tornou-se fácil, em razão do aprimoramento das tecnologias, seja pela criação da imprensa (em todos seus níveis) ou dos sistemas informáticos. As tecnologias influenciaram o modo de viver dos homens, independentemente de sua classe social.

Com efeito, é importante ressaltar que os termos tecnologia e informática não são sinônimos. Tecnologia se refere ao emaranhado de métodos, instrumentos e técnicas produzidas pela ciência e engenharia, cujo objetivo é facilitar o desenvolvimento de atividades, isto é, torna-las mais práticas para o homem.

Por sua vez, a informática trata, especificamente, de mecanismos que influenciam na comunicação, isto é, que viabilizam a troca de informações, que se manifesta em inúmeros âmbitos profissionais, por exemplo, na arte, desenho, vídeo, transporte, telecomunicações, computação, etc.

Dessa maneira, pode-se dizer que a ciência informática está internalizada na tecnologia, tanto que hoje há o que se chama de tecnologia da informação ou TI, caracterizada pelo “conjunto de dispositivos individuais, como hardware, software,

---

[1] Publicação da IBM, 1977, *Apud:* MATTELART, Armand. **A era da informação: gênese de uma denominação descontrolada.** Tradução de Francisco Rüdiger. Revista FAMECOS, Porto Alegre, V. 08, nº. 15, p. 07-23, ago. 2001, p. 07.

telecomunicações ou qualquer outra tecnologia que, faça parte ou gere tratamento da informação ou, ainda, que a contenha".[2]

Nesse sentido, João Araújo Monteiro Neto esclarece que:

> O grande paradigma da história humana moderna consubstancia-se na invenção e no aperfeiçoamento das novas tecnologias surgidas no período pós-industrial que impulsionaram o desenvolvimento de instrumentos que implodiram a realidade humana até então existente. O fator que desencadeou esta transformação foi o surgimento de uma nova tecnologia: a tecnologia da informação. O computador e os sistemas eletrônicos revolucionaram não só o modo de se viver, mas também o de agir do homem.[3]

É inevitável que novas descobertas transformem a sociedade; a tecnologia, por exemplo, nem sempre é benéfica, como se verá no decorrer deste trabalho. Sistemas informatizados são utilizados para prática de delitos. O que deveria ser salutar para o desenvolvimento da sociedade, que anseia por conhecimento, é utilizado por pessoas mal-intencionadas para obterem lucro, prejudicar outrem ou simplesmente por capricho.

Sistemas eletrônicos, tidos incialmente como colaboradores das atividades da sociedade, assumem atualmente o papel fundamental, já que sua presença é de suma importância para o desenvolvimento da vida em sociedade.

Nesse sentido, Monteiro Neto estabelece que:

> O fogo, a roda, a escrita, a moeda, a pólvora, a energia elétrica, as máquinas de calcular, o computador, os sistemas eletrônicos. A evolução do conhecimento humano fez com que a cada nova descoberta a sociedade sofresse transformações nem sempre benéficas. A realidade social pós-industrial parecia estagnada quando o evoluir de um aparelho que simplesmente fazia cálculos modificou de forma profunda e irreversível a vida humana.
> Os sistemas eletrônicos, antes simples coadjuvantes das atividades humanas, hoje assumem papel imprescindível na vida em sociedade moderna, pois está presente de forma direta ou indireta em todas as atividades humanas.[4]

---

[2] CRUZ, Tadeu. **Sistemas, organizações e métodos: estudo integrado das novas tecnologias de informação.** 3. ed. São Paulo: Atlas, 2008, p. 186. *Apud:* MENDONÇA, Cláudio Márcio Campos de. **Sistemas de informação e a gestão da tecnologia da informação.** Disponível em: http://www2.unifap.br/claudiomarcio/files/2014/05/Cap%C3%ADtulo-de-Livro-Temas-em-Gest%C3%A3o-de-TI.pdf. Acessado em: 16 de nov. 2016.

[3] MONTEIRO NETO, João Araújo. **Aspectos constitucionais e legais do crime eletrônico.** 2008. 191 f. Dissertação (Mestrado em Direito Constitucional), Universidade de Fortaleza, 2008, p. 13.

[4] *Ibidem*, p. 14.

No texto “pensar a internet”, Dominique Wolton consigna que a internet deve ser pensada de acordo com sua dimensão técnica, da cultura e da sociedade, bem como ainda é preciso discutir como a revolução da internet afeta o internauta, o indivíduo e o cidadão, tendo em vista a capacidade destrutiva do ser humano; a capacidade de utilizar uma coisa boa em seu desfavor:

> A história ensina que o homem tem sempre uma incalculável capacidade de destruição em si mesmo. Se não se quer que as técnicas mais sofisticadas que o homem inventou sejam a oportunidade para uma nova desumanização, é preciso preservar o homem, suas fraquezas, suas forças e suas contradições. Porque só ele sonha o futuro, pensa sua história e dá sentido a sua experiência.[5]

Com efeito, tratando-se da evolução tecnológica e informática, os principais sistemas informáticos causadores de profundas mudanças no cotidiano das pessoas são o computador e a internet, cuja origem será tratada a seguir.

2.1 HISTÓRIA DO COMPUTADOR

Computador representa um equipamento eletrônico de processamento de dados, o termo computador vem do latim “*computadore”*, ou seja, aquele que realiza cálculos.

Com maior profundidade, Carla Rodrigues de Araújo de Castro conceitua computador:

> (...) como sendo um processador de dados que pode efetuar cálculos importantes, incluindo numerosas operações aritméticas e lógicas, sem a intervenção do operador humano durante a execução. É a máquina ou sistema que armazena e transforma informações, sob o controle de instruções predeterminadas. Normalmente consiste em equipamento de entrada e saída, equipamento de armazenamento ou memória, unidade aritmética e lógica e unidade de controle.[6]

---

[5] WOLTON, Dominique. **Pensar a internet.** Tradução de Daniela Dariano. Revista FAMECOS, Porto Alegre, V. 08, nº. 15, p. 24-28, ago. 2001, p. 28.
[6] CASTRO, Carla Rodrigues Araújo. **Crimes de informática e seus Aspectos Processuais**. 2ª ed. Rio de Janeiro: Lumen Juris, 2003, p. 01.

Destaca-se que a primeira máquina construída para fazer cálculos foi o ábaco, surgida há aproximadamente 2000 anos a.C, sendo conhecida como o primeiro computador.

O computador como conhecemos hoje foi criado na década de 40, durante a Segunda Guerra Mundial. A "*International Business Machines Corporation"* em conjunto com a marinha americana e o grupo Ultra desenvolveram o primeiro computador eletrônico, o qual foi projetado por Haward Aiken e Konrad Zuze, de acordo com o cálculo de Charles Babbage.[7] Ao respectivo computador deu-se o nome de *"*ASSCC - *Automatic Sequence Controlled Calculator"* (Calculadora Automática de Sequência Controlada), mais conhecido como *"MARK I"*.[8]

Não obstante, ainda é difícil estabelecer a paternidade do computador moderno, ora dizem que foi criado por Howard H. Aiken em 1937, ora por John Atasanoff e Berry em 1940, embora a justiça norte-americana o tenha concedido esse título em 1973. Independentemente disso, o fato é que a computação se desenvolveu durante a Segunda Guerra Mundial, como expõe Rossini:

> Não é pacífica a paternidade do moderno computador, ora se dizendo que fora criado por Howard H. Aiken em 1937, ora se afirmando que fora criado por Atasanoff e Berry em 1940. O que fica, entretanto, é que a evolução dessa tecnologia deveu-se ao advento da Segunda Guerra Mundial, que gerou, além de grande desgraça, enorme avanço tecnológico nas mais variadas áreas, inclusive na computação.[9]

Fernando Jose da Costa consigna que existe cinco gerações de computadores, sendo a primeira o desenvolvimento do "*MARK I*" e o *"ENIAC" (Electronic, Numeric, Integrator and Calculator*), criado por John Presper Eckert e John W. Mauchly entre os anos de 1934 e 1946. A segunda geração se manifesta pelo surgimento dos computadores por válvulas eletrônicas em 1951, que armazenava programas dentro da memória interna. Já na década de 60 surgiram os computadores que utilizavam circuitos eletrônicos, ocasião que foram fabricados os microcomputadores. Por sua vez, a quarta geração consagrou-se com o aumento da capacidade de

---

[7] GIMESES, Amanuel Alberto Sperandio Garcia. **Crimes virtuais**. Disponível em: http://bdjur.stj.jus.br/dspace/handle/2011/64929, acesso em: 20 de ago. de 2016.
[8] COSTA, Fernando José da. ***Locus Delicti* nos crimes informáticos.** 2011. 355 f. Tese (Doutorado em Direito) – Faculdade de Direito da USP, São Paulo, 2011, p. 14.
[9] ROSSINI, Augusto Eduardo de Souza. **Informática, Telemática e Direito Penal.** São Paulo: Memória Jurídica Editora, 2004, p. 24.

armazenamento dos computadores. A quinta geração apresenta a evolução dos *hardwares, softwares* e telecomunicações.[10]

Analisando as cinco gerações, Rossini explica que:

> 1ª geração (de 1940 a 1952) – computadores à base de válvulas à vácuo – alimentação por cartões perfurados – uso exclusivamente militar (nessa época surgiu a teoria da "informática jurídica" desenvolvida por Lee Loevinger). 2ª geração (de 1952 a 1964) – substituição das válvulas por transistores – maior velocidade – uso administrativo e gerencial. 3ª geração (de 1964 a 1971) – substituição dos transistores pelos circuitos integrados (surgidos em 1964) – miniaturização dos grandes computadores – evolução dos softwares e criação dos chips de memória – ampliação do uso comercial. 4ª Geração (de 1971 a 1981) – substituição dos circuitos pelos microprocessadores – criação dos floppy disks, ou disquetes, para o armazenamento de dados – nascimento da telemática. 5ª geração (de 1981 até hoje) – enorme avanço da computação – criação da inteligência artificial, da linguagem natural e da altíssima velocidade do processamento de dados – principal novidade: disseminação da internet.

Atualmente, o computador tornou-se um eletrodoméstico indispensável para o desenvolvimento das atividades diárias, cuja utilização facilitou também o exercício das atividades profissionais e empresariais das pessoas.

É preciso registrar que o computador não é o único objeto do crime informático, já que a conduta pode ser perpetrada por celulares, tablets, ipods, etc., entretanto, é umas das principais ferramentas utilizadas pelos criminosos

Com efeito, em que pese a criação dos computadores tenha sido fundamental para o desenvolvimento da tecnológico e social, outra ferramenta foi essencial para a comunidade mundial, a internet, cuja análise será feita a seguir.

2.2 HISTÓRIA DA INTERNET

A internet é uma a rede mundial de comunicações que interliga milhões de computadores e outros equipamentos eletrônicos que possibilitem o acesso, sendo definida pela ANATEL, através da Norma 004/95, que regulamenta o uso dos meios da rede pública de telecomunicações para acesso à internet, como:

> a) Internet: nome genérico que designa o conjunto de redes, os meios de transmissão e comutação, roteadores, equipamentos e protocolos

[10] COSTA, Fernando José da. ***Locus Delicti* nos crimes informáticos.** 2011. 355 f. Tese (Doutorado em Direito) – Faculdade de Direito da USP, São Paulo, 2011, p. 14/15.

> necessários à comunicação entre computadores, bem como o "software" e os dados contidos nestes computadores;

Liliana Minardi Paesani estabelece que não é clara a definição de internet, contudo, analisando-a sob um ponto de vista técnico, é possível esclarecer que:

> (...) a Internet é uma imensa rede que liga elevado número de computadores em todo o planeta. As ligações surgem de várias maneiras: redes telefônicas, cabos e satélites. Sua difusão é levemente semelhante à rede telefônica. Existe, entretanto, uma radical diferença entre uma rede de computadores e uma rede telefônica: cada computador pode conter e fornecer, a pedido do usuário, uma infinidade de informações que dificilmente seriam obtidas por meio de telefonemas.[11]

O início da internet, assim como os computadores, ocorreu em um dos piores momentos vivenciados pela humanidade, dentre testes de bombas nucleares, conflitos e graves crises políticas havidas na década de 50.

Por obra do medo, em 1957 o Departamento de Defesa dos Estados Unidos criou a "*Advanced Research Projects Agency" (ARPA)*, uma agência militar que tinha o objetivo de interligar os departamentos de pesquisa do país. Essa iniciativa foi tomada depois que a União Soviética lançou o primeiro satélite espacial, o Sputnik.

Com efeito, o objetivo da Agência de Investigação de Projetos Avançados era eminentemente militar, de forma que o sistema de telecomunicações preservasse a "corrente de comando dos Estados Unidos", caso fossem atacados.[12]

Emerson Wendt e Higor Vinicius Nogueira Jorge expõem que:

> No ano de 1957 a União Soviética lançou seu primeiro satélite espacial, o Sputnik. A contraofensiva a esse fato foi que o então presidente dos Estados Unidos John Kennedy prometeu enviar um americano para a Lua e criar um sistema de defesa à prova de destruição. Com essa última finalidade e, também, para acelerar o desenvolvimento tecnológico do país e coordenar atividades relacionadas com o espaço e satélites foi criada a Agência de Investigação de Projetos Avançados (*Advanced Research Project Agency* – ARPA).[13]

A ARPA quase foi dissolvida no ano seguinte com a criação da "*National Aeronautics and Space Administration" (NASA)*. Seu funcionamento demandou o

---

[11] PAESANI, Lilian Minardi. **Direito e Internet: liberdade de informação, privacidade e responsabilidade civil.** 6. ed. São Paulo: Atlas, 2013, p. 12.
[12] *Ibidem*, p. 10.
[13] WENDT, Emerson, JORGE, Higor Vinicius Nogiueira. **Crimes cibernéticos: ameaças e procedimentos de investigação.** 2. ed. Rio de Janeiro: Brasport, 2013, p. 05.

reenquadramento de sua missão, alterando o âmbito da pesquisa, que passou a contar com a participação das universidades, atribuindo-lhe uma característica institucional cientifica de renome.

Nesse sentido explica Marcelo Sávio Revoredo Menezes de Carvalho:

> A ARPA, entretanto, quase foi desfeita logo após seu primeiro aniversário, quando seu programa de satélites foi passado para a recém-criada (agência civil) *National Aeronautics and Space Administration* (NASA) e os demais programas de mísseis balísticos passados para outras unidades militares. Para agravar, foi criado, dentro do Departamento de Defesa, um cargo de Diretor de Pesquisa e Engenharia com a missão de coordenar todas as pesquisas militares, inclusive aquelas que estavam designadas à ARPA (NORBERG, O'NEILL, 1996, p. 8). A sobrevivência da ARPA foi possível por meio de um reenquadramento de sua missão, com o reposicionamento do foco no incentivo às pesquisas básicas de longo prazo, através da participação das universidades, que até então estavam fora dos planos do Departamento de Defesa (HAFNER, 1996, p. 22). Essa nova visão da ARPA foi sustentada por Jack Ruina – seu novo diretor –, que a reputou como uma agência de elite, uma instituição cientificamente respeitada, na qual promoveu a descentralização do gerenciamento, valorizando o mérito científico e técnico acima da relevância imediata do objetivo militar.[14]

Em 1966 iniciou-se o estágio de criação da *"Research Projects Angency Network"* (ARPANET), cuja finalidade era interligar os computadores das instituições, contudo, somente em 1969 o sistema foi instalado e passou a operar em quatro computadores de grande porte, em quatro instituições de ensino, conforme descreve Marcelo:

> (...) em primeiro de setembro de 1969, com a universidade praticamente vazia,XIV foi instalado o primeiro IMP e, ao longo do resto do ano, mais três, ficando a ARPANET operacional antes do final da década de sessenta com quatro nós, interconectando os seguintes *mainframes* (computadores de grande porte) através de linhas telefônicas (da AT&T):
>
> - *University of California at Los Angeles* (UCLA), com o computador SDS Sigma 7 rodando o sistema operacional Sigma EXperimental system (SEX). Era o nó responsável pelo gerenciamento da rede;
> - *University of California at Santa Barbara* (UCSB) com o computador IBM 360/75 rodando sistema operacional OS/MVT. Possuía aplicações interativas de matemática para serem compartilhadas;
> - *University of Utah* (UU), com o computador DEC PDP-10 rodando o sistema operacional Tenex. Possuía expertise em computação gráfica.

[14] CARVALHO, Marcelo Sávio Revoredo Menezes de. **A trajetória da internet no Brasil: do surgimento das redes de computadores à instituição dos mecanismos de governança.** 2006. 259 f. Dissertação (Mestrado em Ciências de Engenharia de Sistemas e Computação) – Programa de Pós-graduação de engenharia da Universidade Federal do Rio de Janeiro, 2006, p. 09.

> - *Stanford Research Institute* (SRI)27, com o computador SDS-940 rodando o sistema operacional Genie. Era o nó responsável pelo centro de informações da rede e organizava a distribuição de endereços;[15]

A tecnologia aplicada pela ARPANET para o transporte de informações era chamada de *"packet switching"* ou troca de pacotes. O respectivo autor explica como funciona essa técnica da seguinte forma:

> (...) Nas redes de computadores baseadas nessa técnica, a informação é dividida em pequenas partes (pacotes) antes de ser enviada. Cada pacote carrega o endereço de origem e o de destino, sendo que os pacotes viajam pela rede como unidades independentes de informação, podendo tomar rotas diferentes até o computador de destino, onde são reordenados e checados e a informação é então reconstituída. A comutação de pacotes permite que diversos usuários compartilhem um mesmo canal de comunicação.[16]

Devido ao sucesso, iniciou-se a fase de expansão do sistema, que ganhou novos parceiros após a demonstração realizada durante a primeira "*International Conference on Computer Communications" (ICMM)*, ocorrida em Washington, DC, nos Estado Unidos. Nessa oportunidade, a agência comprovou que as redes funcionavam quando interligou quarenta máquinas.[17]

Os avanços fizeram com que a ARPA chegasse a três redes, a ARPANET, PRNET e SATNET, cujo objetivo passou a ser interconectar as redes heterogêneas, surgindo então o **Projeto Internet**, que culminou na criação de protocolos, chamados de "*Transmission Control Protocol/Intenet Protocol"* (TCP/IP).[18]

O Protocolo de Controle de Transmissão (TCP) possibilita que a informação se mantenha íntegra durante o processo de envio e Protocolo da Internet (IP) é o endereço que assegura aos computadores o acesso a informações, tanto para enviar como receber.

No ano de 1977 o TCP/IP foi demonstrado pela primeira vez, conectando as três redes (ARPANET, SATNET e PRNET), "na qual os pacotes de informação deram voltas de mais de 150 mil km entre as três redes sem perder nenhuma informação".

---

[15] CARVALHO, Marcelo Sávio Revoredo Menezes de. **A trajetória da internet no Brasil: do surgimento das redes de computadores à instituição dos mecanismos de governança.** 2006. 259 f. Dissertação (Mestrado em Ciências de Engenharia de Sistemas e Computação) – Programa de Pós-graduação de engenharia da Universidade Federal do Rio de Janeiro, 2006, p. 19.
[16] *Ibidem*, p. 11.
[17] *Ibidem*. p. 20/21.
[18] WENDT, Emerson, JORGE, Higor Vinicius Nogiueira. **Crimes cibernéticos: ameaças e procedimentos de investigação.** 2. ed. Rio de Janeiro: Brasport, 2013, p. 07.

Com isso, o incentivo militar aumentou e o sistema foi financiado, porém a internet civil só passou a se desenvolver, quando houve a separação da rede militar da ARPANET.[19]

Já na década de 80, mais precisamente em 1985, após investimento da "*National Science Foundation" (NSF)*, nasce o "*National Science Foundation Network"* (NSFNET). Segundo Costa, a internet surgiu com a ligação dos *backbone* NTF com a ARPANET, sendo *backbone*, a "espinha dorsal dos cabos de telecomunicação entre computadores (...) possibilitando a visualização e a transferência de dados através de quilômetros de distância".[20]

O sistema pioneiro (ARPANET) deixou de existir 1990 devido a criação de outras redes, sendo que em 1993, com a criação da "*World Wide Web" (www)* a internet passou a ser comercializada, nascendo definitivamente o "mundo *online*".[21]

Nesse seguimento, Paesani disserta que:

> O mais importante elemento, detonador dessa verdadeira explosão, que permitiu à Internet se transformar num instrumento de comunicação de massa, foi o *World Wide Web* (ou *WWW*, ou ainda W3, ou simplesmente *Web*), a rede mundial.
> O WWW nasceu no ano de 1989 no Laboratório Europeu de Física de altas energias, com sede em Genebra, sob o comando de T. Berners-Lee e R. Cailliau. É composto por hipertextos, ou seja, documentos cujo texto, imagem e sons são evidenciados de forma particular e podem ser relacionados com outros documentos. Com um clique no *mouse* o usuário pode ter acesso aos mais variados serviços, sem necessidade de conhecer os inúmeros protocolos de acesso.[22]

Feita essa breve contextualização histórica, importa também demonstrar como a internet chegou ao Brasil.

---

[19] CARVALHO, Marcelo Sávio Revoredo Menezes de. **A trajetória da internet no Brasil: do surgimento das redes de computadores à instituição dos mecanismos de governança.** 2006. 259 f. Dissertação (Mestrado em Ciências de Engenharia de Sistemas e Computação) – Programa de Pós-graduação de engenharia da Universidade Federal do Rio de Janeiro, 2006, p. 24/27.
[20] COSTA, Fernando José da. ***Locus Delicti* nos crimes informáticos.** 2011. 355 f. Tese (Doutorado em Direito) – Faculdade de Direito da USP, São Paulo, 2011, p. 23.
[21] *Ibidem*, p. 23.
[22] PAESANI, Lilian Minardi. **Direito e Internet: liberdade de informação, privacidade e responsabilidade civil.** 6. ed. São Paulo: Atlas, 2013, p. 11.

2.3 A INTERNET NO BRASIL

A história do surgimento da internet no Brasil não é muito extensa. A internet chegou no Brasil ainda na década de 80, contudo, seu objetivo era estritamente acadêmico. O que proporcionou isso foi o sistema de rede denominado "*Because It's Time Network"* (BITNET), fundado em 1981 e fazia ligação entre a *City University of New York* (CUNY) e *Yale University*, em Connecticut. O sistema conectou em 1988 a Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) ao *Fermi National Laboratory* (Fermilab), laboratório de física, localizado em Batavia, Illinois, nos Estados Unidos, sendo que no final desse mesmo ano, outras quatro instituições de ensino do Estado de São Paulo estariam conectadas (USP, INICAMP, UNESP e IPT).[23]

O Ministério da Ciência e Tecnologia criou em 1990 a Rede Nacional de Pesquisa (RNP), cuja função era implementar os serviços de internet no país, sendo que em 1992 o sistema interligou 11 capitais brasileiras, conectando universidades, centros de pesquisa e organizações não governamentais do país.[24]

É necessário registrar ainda que a Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP) foi a primeira encarregada com o domínio ".br" e da distribuição dos números de IPs no país.

Outrossim, a internet ganhou o público geral em 1994 com a EMBRATEL, que disponibilizou a cinco mil pessoas o serviço de conexão experimental.

> A Embratel iniciou seu serviço de acesso à Internet via linha discada (14.400 bps) em caráter experimental em dezembro de 1994, por meio de um teste com um pequeno grupo de usuários (EMBRATEL, 1994). Essa primeira fase do projeto foi feita com o apoio da RNP, uma vez que a Embratel não possuía recursos humanos e infraestrutura de equipamentos para prover serviços de Internet. A segunda fase do projeto compreenderia a distribuição gradativa da conexão à rede aos cerca de quinze mil usuários antecipadamente cadastrados para participar. O plano da Embratel era atender, em média, quinhentas pessoas por semana até suprir toda a demanda. A segunda fase do projeto começou efetivamente em maio de 1995, quando a Embratel passou a oferecer o serviço de acesso à Internet através do acesso ao *Global Internet Exchange* (GIX) que provia acesso CIX nos Estados Unidos. A Embratel anunciou também que os usuários do seu serviço STM-400

[23] CARVALHO, Marcelo Sávio Revoredo Menezes de. **A trajetória da internet no Brasil: do surgimento das redes de computadores à instituição dos mecanismos de governança.** 2006. 259 f. Dissertação (Mestrado em Ciências de Engenharia de Sistemas e Computação) – Programa de Pós-graduação de engenharia da Universidade Federal do Rio de Janeiro, 2006, p. 84/85.
[24] COSTA, Fernando José da. ***Locus Delicti* nos crimes informáticos.** 2011. 355 f. Tese (Doutorado em Direito) – Faculdade de Direito da USP, São Paulo, 2011, p. 24.

> poderiam enviar e receber mensagens de correio eletrônico da Internet e fazer FTP-Mail, bem como poderiam ter acesso, via RENPAC, às aplicações de FTP, Telnet e Gopher.[25]

No ano seguinte, em 1995, a internet saiu do meio acadêmico e passou a ser disponibilizada e comercializada para as demais áreas da sociedade.

> Mais precisamente em maio de 1995, a operação da Rede no Brasil deixou de atuar nas áreas da educação e pesquisa, para tornar-se acessível comercialmente a qualquer setor da sociedade, com a criação de um provedor de acesso privado.[26]

Com efeito, hoje o Brasil conta com milhares de internautas e a cada dia mais e mais pessoas iniciam seu acesso à rede, seja pelos computadores, tablets, celulares, etc.[27] O mesmo ocorre com a criação de *sites*, que também aumenta diariamente.

Em oposição aos benefícios que a internet trouxe para o país, houve o crescimento da criminalidade, agora informatizada. Exposto isso, é fundamental demonstrar qual a relação havida entre o Direito e a internet.

2.4 DIREITO E A INFORMATIZAÇÃO

A nova era galgou avanços tecnológicos absurdos, que provocaram mudanças na sociedade, notadamente com o surgimento dos computadores e da internet. É patente a ocorrência de uma transformação social, que se manifesta em inúmeros ramos, por exemplo, na educação, cultura, economia, etc.

Como não poderia ser diferente, o direito é diretamente provocado pelos respectivos avanços, tendo em vista a necessidade de atribuir segurança jurídica as novas relações jurídicas, decorrentes do processo tecnológico, em outras palavras,

---

[25] CARVALHO, Marcelo Sávio Revoredo Menezes de. **A trajetória da internet no Brasil: do surgimento das redes de computadores à instituição dos mecanismos de governança.** 2006. 259 f. Dissertação (Mestrado em Ciências de Engenharia de Sistemas e Computação) – Programa de Pós-graduação de engenharia da Universidade Federal do Rio de Janeiro, 2006, p. 137.

[26] COSTA, Fernando José da. ***Locus Delicti* nos crimes informáticos.** 2011. 355 f. Tese (Doutorado em Direito) – Faculdade de Direito da USP, São Paulo, 2011, p. 24.

[27] As pesquisas indicam que mais de 50% (cinquenta por cento) da população brasileira faz uso da internet. (http://g1.globo.com/tecnologia/noticia/2016/04/internet-chega-pela-1-vez-mais-de-50-das-casas-no-brasil-mostra-ibge.html)

os novos bens jurídicos carecem de tutela,[28] cujo vácuo pode ocasionar problemas difíceis de serem reparados.

O desenvolvimento trouxe consigo uma nova sociedade, com novos interesses, técnicas e até litígios. E é justamente por isso que o Direito não pode eximir-se de sua responsabilidade e deve acompanhar os novos anseios sociais, visando, primordialmente, tutelar os bens tidos como fundamentais.

Sobre isso, Norberto Bobbio já dizia que:

> Não e preciso muita imaginação para prever que o desenvolvimento da técnica, a transformação das condições econômicas e sociais, a ampliação dos conhecimentos e a intensificação dos meios de comunicação poderão produzir tais mudanças na organização da vida humana e das relações sociais que se criem ocasiões favoráveis para o nascimento de novos carecimentos e, portanto, para novas demandas de liberdade e de poderes. Para dar apenas alguns exemplos, lembro que a crescente quantidade e intensidade das informações a que o homem de hoje está submetido faz surgir, com forca cada vez maior, a necessidade de não se ser enganado, excitado ou perturbado por uma propaganda maciça e deformadora; começa a se esboçar, contra o direito de expressar as próprias opiniões, o direito a verdade das informações. No campo do direito a participação no poder, faz-se sentir na medida em que o poder econômico se torna cada vez mais determinante nas decisões políticas e cada vez mais decisivo nas escolhas que condicionam a vida de cada homem — a exigência de participação no poder econômico, ao lado e para além do direito (já por toda parte reconhecido, ainda que nem sempre aplicado) de participação no poder político. O campo dos direitos sociais, finalmente, está em continuo movimento: assim como as demandas de proteção social nasceram com a revolução industrial, e provável que o rápido desenvolvimento técnico e econômico traga consigo novas demandas, que hoje não somos capazes nem de prever.[29]

Com efeito, o Direito está em constante mutação do mesmo modo que a sociedade, e não consegue acompanhar as transformações sociais, contudo, ainda assim, não pode permanecer estático.

Monteiro Neto explique que o Direito é estanque e por isso não consegue acompanhar os mesmos níveis de transformação da sociedade, no entanto, ressalta que o Direito pode responder as novas necessidades após sua assimilação com o novo:

---

[28] MONTEIRO NETO, João Araújo. **Aspectos constitucionais e legais do crime eletrônico.** 2008. 191 f. Dissertação (Mestrado em Direito Constitucional), Universidade de Fortaleza, 2008, p. 50.
[29] BOBBIO, Norberto. **A era dos direitos**. Tradução de Carlos Nelson Coutinho, apresentação de Censo Lafer. Nova ed. Rio de Janeiro: Elsevier, 2004, 7ª reimpressão, p. 33.

> O direito posto de forma concreta, por ser estanque, não pode acompanhar em nível de igualdade as transformações sociais decorrentes do avanço tecnológico. Mas nem por esse motivo pode o Direito ficar inerte. Inúmeras são as situações em que o Direito foi impactado por novos fenômenos jurídicos e que após a assimilação desses novos contextos consegue responder aos anseios sociais de regulamentação.[30]

Registra-se que o Estado, enquanto agente detentor do Poder Público, deve cumprir com primazia suas funções de maneira que preserve e garanta aos membros da sociedade, seus direitos e preceitos fundamentais que amparam sua própria existência. A internet não pode promover uma autorregulamentação, já que isso é obrigação do ente Estatal que, em tese, conhece as necessidades da sociedade, haja vista saber das condutas proibidas e obrigatórias que carece de regulamentação.

Assim como aconteceu com outras áreas jurídicas, o Direito Penal sofreu intensas influências com o surgimento da internet, pois embora não tenha sido criada para viabilizar a prática de ações criminosas, é o que vem ocorrendo.

Greco Filho acredita que a internet é somente mais uma faceta da criatividade do homem, e, portanto, deve ser tutelada pelo direito, todavia, essa tutela não pode ocorrer apressadamente. Segundo o autor, a ordem jurídica atual existente é plenamente capaz de disciplinar a nova realidade social, sem a necessidade realizar qualquer modificação.

> A internet não passa de mais uma pequena faceta da criatividade do espírito humano e como tal deve ser tratada pelo direito, especialmente o penal. Evoluir, sim, mas sem querer "correr atrás", sem se precipitar e, desde logo, afastando a errônea ideia de que a ordem jurídica desconhece ou não está apta a disciplinar o novo aspecto da realidade. E pode fazê-lo no maior número de aspectos, independentemente de qualquer modificação.[31]

Não obstante, o Direito Penal ainda não é capaz de tutelar todas as condutas criminosas praticadas através de meios eletrônicos, pois ações como a distribuição de cavalos de Troia, vírus eletrônicos e "*worms"* ainda não estão regulamentadas.

É certo que a efetividade do Direito Penal depende da capacidade que tem de desempenhar suas funções, por isso que o ordenamento jurídico deve se amoldar a

---

[30] MONTEIRO NETO, João Araújo. **Aspectos constitucionais e legais do crime eletrônico.** 2008. 191 f. Dissertação (Mestrado em Direito Constitucional), Universidade de Fortaleza, 2008, p. 51.
[31] GRECO FILHO, Vicente. **Algumas observações sobre o direito penal e a Internet**. Boletim IBCCRIM, ano 8, nº. 95, out. 2000.

nova realidade social, cuja adaptação garante sua própria existência[32], conforme ensina Eugênio Raúl Zaffaroni e José Henrique Pierangeli:

> A *efetividade* do direito penal é sua capacidade para desempenhar a função que lhe incumbe no atual estágio de nossa cultura. Esta função é a de garantia externa de um âmbito de autorrealização humana, isto é, a garantia de disponibilidade daquilo que se considera que pode ser necessário para realizar-se em coexistência (para escolher ser o que se quer ser). Logo, é efetivo o direito penal capaz de servir de garantia externa da existência.
> Um direito penal que não tenha esta capacidade será *não efetivo,* e gerará tensões sociais e conflitos que acabarão destruindo sua eficácia (vigência). Não obstante, continuará sendo direito penal e estará vigente enquanto for sustentado.[33]

E mais, segundo os autores, o Direito Penal sem efetividade representará somente um mero exercício de poder e para que haja essa efetividade, é fundamental que respeite as condições humanas, caso contrário, não passará de um direito penal repressor, terminando em um “espetáculo para sádicos” Eis o que dizem:

> Se a carência de efetividade é de grau tão elevado, que afeta o atual horizonte de projeção da ciência jurídico-penal, este ficará reduzido a um simples exercício de poder e não será direito penal.
> Para que o direito penal tenha efetividade, será necessário que respeite a condição humana: que sirva ao homem a partir de um reconhecimento do ser do homem. *Isto é a fundamentação antropológica.* O direito penal efetivo deverá estar antropologicamente fundamentado. O direito penal não efetivo não o estará, mas continuará sendo direito penal enquanto conserve eficácia. O mero exercício de poder durará enquanto durar a sua eficácia, mas não será direito penal e estará ainda mais distante da fundamentação antropológica do que o direito penal não efetivo.
> (...)
> O direito penal efetivo será aquele que tenha capacidade para mostrar-se como um direito penal "liberador", enquanto o não efetivo será um direito penal "repressivo". Aqueles que afirmam que todo direito penal é repressivo porque "reprime" caem num absurdo infantilismo positivista, cômodo para quem detém o poder, até o dia em que seja deposto por seu opositor. Tudo se passará da mesma maneira como critério acerca do "repressivo" fundado no formal: nós, cientistas do direito penal, nos sentaremos para presenciar como aquele que tem o poder fuzila seus opositores e, no dia seguinte, como os opositores de ontem fuzilam os depostos de hoje. O direito penal pode terminar em um espetáculo para sádicos.[34]

---

[32] CONTE, Christiany Pegorari. **Jurisdição e competência nos crimes informáticos.** Revista Brasileira de Meio Ambiente Digital e Sociedade da Informação. V. 01, nº. 01, p. 49-208, 2014, p. 53.
[33] ZAFFARONI, Eugênio Raúl, PIERANGELI, José Henrique. **Manual de direito penal brasileiro: volume 01: parte geral.** 9. ed. rev. e atual. São Paulo: Editora Revista dos Tribunais, 2011, p. 321.
[34] *Ibidem*, p. 321/323.

À vista disso, o Brasil precisa adequar a legislação com a finalidade de restringir a violação de direitos fundamentais dos cidadãos, de maneira que lesões e ameaças à liberdade, bem como ao próprio interesse público, sejam rechaçados.[35]

Embora a legislação ainda seja carente, a doutrina começou a estudar os crimes informáticos, a fim de viabilizar sua compreensão e criminalização, cujos aspectos serão analisados no próximo capítulo.

[35] FERREIRA LIMA, Paulo Marco. **Bem jurídico e os crimes de computador**. Revista Justitia, São Paulo, V. 197, p. 381-385, jul/dez. 2007, p. 383.

3 CRIMES INFORMÁTICOS

Como visto, o avanço tecnológico trouxe consigo algumas adversidades, consistentes na prática de condutas criminosas, que ocorrem a partir da utilização de sistemas eletrônicos que estão ligados à rede mundial de computadores (*internet*).

Assim, é fundamental definir o crime, de forma que seja plenamente visível sua prática, bem como suas classificações e espécies, cuja análise será realizada neste capítulo.

3.1 CONCEITO

É fato que a *internet* mudou o mundo, trazendo consigo inúmeras facilidades, principalmente no que diz respeito a busca por conhecimento, bem como a comunicação.

Ocorre que as condutas praticadas no meio virtual transpassam para o real, viabilizando acontecimentos e consequências, inclusive, de cunho criminal, fato que demonstra o quão importante é direito penal.

Isso acontece porque além de benefícios, a internet angariou ferramentas práticas para que criminosos cometam delitos. Essas transgressões se traduzem não só nas condutas positivadas na atual legislação, como aquelas que carecem de positivação, que tolhem a preservação do bem jurídico alheio.

Sobre isso, Reginaldo César Pinheiro preleciona que:

> Com a popularização da Internet em todo o mundo, milhares de pessoas começaram a se utilizar deste meio. Contemporaneamente se percebe que nem todos a utilizam de maneira sensata e, acreditando que a internet é um espaço livre, acabam por exceder em suas condutas e criando novas modalidades de delito: os crimes virtuais.[36]

A classificação legal ou *"nomen iuris"* de um crime é fundamental para a boa compreensão da conduta, cuja técnica foi adotada pela legislação para denominar a figura criminosa.

---

[36] PINHEIRO, Reginaldo César. **Os Crimes Virtuais na esfera jurídica brasileira**. **Boletim IBCCrim.** Ano 8, n 101, abril/2001, p. 18.

Fragoso consigna que:

> A classificação dos crimes na parte especial do código é questão de técnica legislativa, e é feita com base no bem jurídico tutelado pela lei penal, ou seja, a objetividade jurídica dos vários delitos ou das diversas classes de intenções[37].

Sobre isso, Rogério Sanches Cunha explica o seguinte:

> A classificação legal diz respeito ao nomen iuris, ou seja, à denominação que a própria lei confere à figura criminosa, etiquetando os tipos penais. Ex.: homicídio, furto, estupro, peculato. São todas denominações que a lei se encarrega de estabelecer.[38]

Ocorre que os estudiosos divergem quanto a nomenclatura utilizada para as condutas criminosas praticadas com o auxílio da informática. São inúmeros os termos utilizados, por exemplo: cibercrimes, delitos cibernéticos ou informáticos, crimes virtuais, criminalidade de computador, crimes de computador, crimes de internet, etc.

Não obstante, independentemente da terminologia adotada, todos tratam da respectiva conduta criminosa, embora algumas definições não representem todas as dimensões do crime.

A professora Ivette Senise Ferreira, citada por Neto e Guimarães, expõe que os crimes da informática são "toda ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão"[39].

Por sua vez, o Promotor de Justiça Augusto Eduardo de Souza Rossini, disserta que delitos informáticos são aqueles cuja conduta é desempenhada tanto no âmbito da internet, como aqueles que vinculam o uso de sistemas informáticos:

> (...) "delitos informáticos" alcança não somente aquelas condutas praticadas no âmbito da internet, mas toda e qualquer conduta em que haja relação com sistemas informáticos, quer de meio, quer de fim, de modo que essa

---

[37] FRAGOSO, Heleno Cláudio. **Lições de direito penal: parte especial: arts. 121 a 212 do CP.** Rio de Janeiro: Forense, 1983, p. 05. *Apud:* VIANNA, Túlio Lima. **Do acesso não autorizado a sistemas computacionais: fundamentos de direito penal informático.** 2001. 241 f. Dissertação (Mestrado em Direito) – Faculdade de Direito da UFMG, Belo Horizonte, 2001, p. 31.

[38] CUNHA, Rogério Sanches. **Manual de direito penal – parte geral (arts. 1º ao 120).** 3 ed. rev. ampl. e atual. Salvador/BA: JusPODIVM, 2015, p. 159.

[39] FERREIRA, Ivette Senise. **A criminalidade informática**. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto (coord.). **Direito e internet: aspectos jurídicos relevantes**. Bauru: Edipro, 2000. p. 207 – 237, p. 210. *Apud*: NETO, Mário Furlaneto, GUIMARÃES, José Augusto Chaves. **Crimes na internet: elementos para uma reflexão sobre a ética informacional.** Periódico do Conselho da Justiça Federal, Brasília, V. 07, nº. 20, p. 67-73, jan./mar. 2003, p. 69.

> denominação abrangeria, inclusive, delitos em que o computador seria uma mera ferramenta sem imprescindível "conexão" à Rede Mundial de Computadores, ou qualquer outro ambiente telemático.[40]

Em análise as denominações, Túlio Lima Vianna consigna que o termo delitos virtuais não está correto, já que não é possível falar em bem jurídico virtual. Entende que essas condutas criminosas só podem ser chamadas de delitos informáticos ou crimes informáticos, já que o bem juridicamente protegido é a inviolabilidade das informações, cuja conclusão extraiu do próprio conceito de informática. Eis o que expõe:

> Vê-se desde já que a denominação "delitos virtuais" é completamente absurda, pois, anda que se conceba que os delitos são praticados num mundo "virtual", não haveria qualquer sentido em se falar de um bem jurídico virtual.
> (...)
> A ciência que tem como objeto de estudo as informações autorizadas (dados) é a Informática.
> A informática é a ciência que estuda os meios para armazenar, processar e transmitir dados, isto é, para registrar, manipular e transmitir informações de forma autorizada.
> (...)
> Assim, está claro que a denominação mais precisa para os delitos ora em estudo é "crimes informáticos" ou delitos informáticos", por basear-se no bem jurídico penalmente tutelado, que é a inviolabilidade das informações autorizadas (dados).[41]

Paulo Marco Ferreira Lima, prefere utilizar o termo Crimes de Computador, já que o objeto é utilizado para a prática da conduta ilícita.[42]

Para Sergio Marcos Roque crimes de informática são "toda conduta, definida em lei como crime, e em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material"[43].

Com efeito, conquanto a definição do Ferreira Lima está corretíssima, dizer que esses atos ilícitos são praticados somente com o uso de computadores não é certo,

---

[40] ROSSINI, Augusto Eduardo de Souza. **Informática, Telemática e Direito Penal.** São Paulo: Memória Jurídica Editora, 2004, p. 110.
[41] VIANNA, Túlio Lima. **Do acesso não autorizado a sistemas computacionais: fundamentos de direito penal informático.** 2001. 241 f. Dissertação (Mestrado em Direito) – Faculdade de Direito da UFMG, Belo Horizonte, 2001, p. 32/33.
[42] LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional**, Campinas, São Paulo: Millennium, 2005, p. 24. *Apud*: COSTA, Fernando José da. ***Locus Delicti* nos crimes informáticos.** 2011. 355 f. Tese (Doutorado em Direito) – Faculdade de Direito da USP, São Paulo, 2011, p. 52.
[43] ROQUE, Sérgio Roque. **Criminalidade Informática – Crimes e Criminosos do Computador.** 1 ed. São Paulo: ADPESP Cultural, 2007, p. 25.

tendo em vista que o patente avanço tecnológico fez surgir outros mecanismos/aparelhos (*smartphones, tablet, notbook, ipad* etc.) que propiciam ao mal-intencionado a prática criminosa.

Outrossim, a ciência da computação tem como base de estudos os programas de computadores e o bem jurídico tutelado pelo Estado não se refere somente a inviolabilidade de programas[44].

Nesse sentido, é o entendimento de Fernando José da Costa:

> Entendemos imprecisa a definição "crimes de computador". Nos dias atuais, o delito informático não está mais restrito ao uso de um tradicional computador com seu disco rígido, teclado e visor, mas pode ser praticado por diversos outros aparelhos ligados à *internet* como telefone fixo ou móvel, *ipad, loptop, notebook*. Mais adequada, portanto, a nomenclatura "crimes informáticos".[45]

É possível observar que não há concordância entre os estudiosos quanto ao termo utilizado, em razão da dificuldade que se tem de conceituar tais condutas criminosas.

Assim, com finalidade meramente didática, será utilizado o termo Crimes Informáticos quando nos referirmos a

> (...) conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade e a confidencialidade.[46]

Diante disso, passa-se a análise dos bens jurídicos tutelados pelos crimes informáticos.

---

[44] VIANNA, Túlio Lima. **Do acesso não autorizado a sistemas computacionais: fundamentos de direito penal informático.** 2001. 241 f. Dissertação (Mestrado em Direito) – Faculdade de Direito da UFMG, Belo Horizonte, 2001, p. 32.

[45] COSTA, Fernando José da. ***Locus Delicti* nos crimes informáticos.** 2011. 355 f. Tese (Doutorado em Direito) – Faculdade de Direito da USP, São Paulo, 2011, p. 52.

[46] ROSSINI, Augusto Eduardo de Souza. **Informática, Telemática e Direito Penal.** São Paulo: Memória Jurídica Editora, 2004, p. 110.

3.2 BEM JURÍDICO

O direito penal, como ramo jurídico do ordenamento jurídico brasileiro, tem o objetivo de proteger bens e valores da comunidade, preservando aquilo que é essencial para seu desenvolvimento.

Com efeito, esse ramo jurídico possui intima relação com a Constituição Federal, em especial, quando ao resguardo dos bens jurídicos fundamentais, como ensina Luiz Régis Prado:

> A Constituição, como marco fundante de todo ordenamento jurídico, irradia sua forca normativa para todos os setores do Direito. Todavia, tem ela particular e definitiva influencia na seara penal.
> Isso porque cabe ao Direito Penal a proteção de bens e valores essenciais a livre convivência e ao desenvolvimento do individuo e da sociedade, insculpidos na Lei Fundamental, em determinada época e espaço territorial. A relação entre a Constituição e o subsistema penal é tão estreita que o bem jurídico-penal tem naquela suas raízes materiais. E fundamental, inclusive para a salvaguarda dos direitos fundamentais, para que a interpretação e aplicação da lei penal seja feita sempre conforme a Constituição e os ditames do Estado democrático de Direito.[47]

Do mesmo modo, Nilo Batista consigna que o direito penal tem como missão resguardar os bens jurídicos da sociedade.[48] Mas o que são bens jurídicos?

Bem jurídico penal simboliza tudo aquilo que é essencial ao convívio da sociedade, abarcando os direitos individuais e sociais fundamentais. A Constituição Federal ilustra inúmeros bens jurídicos que foram tutelados pelo direito penal, por exemplo, vida, liberdade, igualdade, honra, vida privada, patrimônio, etc.

Sem embargo, cabe consignar que nem tudo será objeto de tutela penal, isto é, nem todos os bens jurídicos serão atingidos pela tutela do direito penal, em razão da intervenção mínima, pressuposto fundamental do ordenamento jurídico penal.

A interferência do Direito Penal na vida da sociedade deve ser mínima, isto é, só deve ser chamado a se manifestar quando os demais ramos do Direito não conseguirem proteger os bens jurídicos. Significa dizer que o Direito Penal deverá se

---

[47] PRADO, Luiz Regis. **Curso de direito penal brasileiro – vol. 1 - parte geral: arts. 1º ao 120.** 9 ed. rev. atual. e ampl. São Paulo: Revistas dos Tribunais. 2010, p. 68.
[48] BATISTA, Nilo. **Introdução crítica ao direito penal brasileiro**. 11 ed. Rio de Janeiro: Revan. 2007, p. 116.

preocupar com a tutela de bens jurídicas de maior importância para a sociedade, como a vida, a liberdade, a dignidade sexual, etc.

Sobre isso o professor Guilherme de Souza Nucci explica que:

> O termo *bem* indica, sempre, algo positivo, como um favor, uma benesse, um proveito ou uma ventura. Por outro lado, num prisma material, aponta para algo apto a satisfazer as necessidades humanas, integrando seu patrimônio. Quando se fala em bem comum, denota-se o nível das condições favoráveis ao êxito coletivo. Em suma, o bem se apresenta vinculado aos mais preciosos interesses humanos, seja do ponto de vista material, seja do prisma incorpóreo (moral ou ético).
> Há bens tutelados pelo Direito, eleitos pelo ordenamento jurídico como indispensáveis à vida em sociedade, merecendo proteção e cuidado. A partir dessa escolha, o bem se transforma em *bem jurídico*. Dos mais simples aos mais complexos; dos inerentes à natureza humana às criações alternativas da vida moderna; dos ligados à dignidade humana aos vinculados a puros interesses materialistas; todos os bens jurídicos gozam do amparo do Direito. Os mais relevantes e preciosos atingem a tutela do Direito Penal, sob a ótica da intervenção mínima. "Nem todo bem jurídico requer tutela penal, nem todo *bem jurídico* há de se converter em um *bem jurídico-penal*" (Mir Puig, *Estado, pena y delito*, p. 85 – traduzi).
> Por isso, quando o bem jurídico penal é destacado como tal, surgem tipos penais incriminadores para protegê-los, indicando as condutas proibidas, sob pena de lesão ao referido bem jurídico tutelado.[49]

É possível verificar que os crimes informáticos lesionam inúmeros bens jurídicos, contudo, no começo esses crimes tinha o objetivo de violar a intimidade das pessoas (físicas ou jurídicas), bem como ferir a honra.

Ocorre que, agora, é possível verifica que os criminosos passaram a lesar outros bens jurídicos, inclusive aqueles de maior importância, como a vida por exemplo. Delinquentes estão usando a internet para proliferar pornografia infantil, aliciar menores para prostituição, praticar crimes contra o patrimônio, etc.

3.3 CLASSIFICAÇÃO

Com o desenvolvimento da criminalidade, a legislação e a doutrina também precisa evoluir a fim de coibir as condutas. Por isso que para analisar com maior profundidade as condutas ilícitas praticas pelos meios informáticos, a doutrina os classificou.

---

[49] NUCCI, Guilherme de Souza. **Manual de direito penal**. 7 ed. rev., atual. e ampl. Rio de Janeiro: Revista dos Tribunais, 2011, p. 69/70.

Assim como ocorre com a definição, a classificação dos crimes informáticos não uníssona, havendo divergências entre os doutrinadores. Parte dos estudiosos classificam em puros, mistos e comuns, outros em próprios, impróprios, mistos, mediatos ou indiretos.

Em que pese as classificações sejam diferentes, seus significados são bem parecidos, como será possível observar.

Pinheiro explique que **crimes informáticos puros ou próprios** representam toda conduta ilícita, cujo objetivo seja atentar contra o sistema de computador, os componentes, sistemas e dados. Ao passo que **crimes informáticos mistos** são aqueles cujo uso da internet é fundamental para realização do crime, sendo o bem jurídico violado diverso do informático. Por fim, **crimes informáticos comuns ou impróprios** se referem aos delitos tipificados na lei penal (ameaça, pornografia infantil, estelionato, etc.), que são praticados com o uso da internet.[50]

Utilizando a denominação crimes virtuais, Christiany Pegorari Conte ensina o seguinte:

> Logo, os crimes virtuais puros são aqueles que atacam o sistema informático *software* (ou programa informático)*, hardware* (que corresponde à parte física do computador, tais como: CPU, monitor, teclado, circuito), dados, sistemas e meios de armazenamento e etc. Já em relação aos crimes mistos, o computador constitui condição sem a qual não seria possível a prática do crime, tais como *a transferência ilícita de valores em uma 'homebanking' ou a prática de 'salemislacing'* (retirada diária de pequenas quantias em milhares de contas, também conhecido como retirada de saldo). Finalmente, os crimes comuns seriam aqueles que já encontram respaldo na legislação brasileira, constituindo, a rede mundial de computadores, apenas mais um meio de execução destes delitos, tal como ocorre nos seguintes crimes, já tipificados pela lei penal: estelionato (art. 171, CP), a ameaça (art. 147, CP), os crimes contra a honra (arts. 138-140, CP), o homicídio (art. 121, CP), veiculação de pornografia infantil (artigo 241, do Estatuto da Criança e do Adolescente - ECA - Lei 8.069/90), crime de violação direito autoral (art. 184, do Código Penal) e etc.[51]

Quanto aos **delitos informáticos impróprios**, em que o computador é usado para a prática da conduta criminosa, Vianna expõe que a consumação do crime independe de conhecimento técnicos por parte do sujeito ativo. Assim leciona:

---

[50] PINHEIRO, Reginaldo César. **Os Crimes Virtuais na esfera jurídica brasileira**. **Boletim IBCCrim.** Ano 8, n 101, abril/2001, p. 19. *Apud:* CONTE, Christiany Pegorari. **Jurisdição e competência nos crimes informáticos.** Revista Brasileira de Meio Ambiente Digital e Sociedade da Informação. V. 01, nº. 01, p. 49-208, 2014, p. 113.

[51] CONTE, Christiany Pegorari. **Jurisdição e competência nos crimes informáticos.** Revista Brasileira de Meio Ambiente Digital e Sociedade da Informação. V. 01, nº. 01, p. 49-208, 2014, p. 113.

> Delitos informáticos impróprios são aqueles no quais o computador é usado como instrumento para a execução do crime, mas não há ofensa ao bem jurídico inviolabilidade da informação autorizada (dados).
> Sua popularidade é grande e, na maioria das vezes, para seu cometimento não há necessidade que o agente detenha grandes conhecimentos técnicos do uso de computador.
> Hipótese clássica de crimes informáticos impróprios são os crimes contra a honra – calúnia (art. 138 CP), difamação (art. 139 CP), injúria (art. 140 CP) – cometidos pelo simples envio de um email.[52]

Ademais, os **crimes informáticos mediatos ou indiretos**, são representados pelo delito-fim, que adquiriu essa característica devido ao delito-meio informático que foi fundamental para sua consumação, ou seja, o delito-fim que não é informático consumou-se em detrimento da prática de uma conduta ilícita antecedente com a utilização de meios informáticos.

Tem-se aqui a conhecida aplicação do princípio da consunção, em que se descarta a delito-meio, pois foi absorvido pelo delito-fim.

Greco leciona que o princípio da consunção se manifesta em duas oportunidades, "quando um crime é meio necessário ou normal fase de preparação ou de execução de outro crime" ou "nos casos de antefato e pós-fato impuníveis".[53] Consigna ainda que:

> (...) consumação absorve a tentativa e esta absorve o incriminado ato preparatório; o crime de lesão absorve o correspondente crime de perigo; o homicídio absorve a lesão corporal; o furto em casa habitada absorve a violação de domicílio etc.[54]

Com efeito, tratando do princípio, Nélson Hungria, expõe brilhantemente que:

> (...) uma norma se deve reconhecer *consumida* por outra quando o crime previsto por aquela não passa de uma *fase de realização* do crime previsto por esta, ou é uma necessária ou normal forma de transição para o último (*crime progressivo)*. O crime previsto pela norma *consuntiva* representa a etapa mais avançada na efetuação do malefício, aplicando-se, então, o princípio de que *major absorbet minorem*. Os fatos, aqui, também não se acham em relação de *species a genus*, mas de *minus a plus*, de parte a todo, de meio a fim. Exemplos: a *consumação* absorve a *tentativa*, e esta absorve o incriminado *ato preparatório;* o *crime de lesão* absorve o *correspondente*

---

[52] VIANNA, Túlio Lima. **Do acesso não autorizado a sistemas computacionais: fundamentos de direito penal informático.** 2001. 241 f. Dissertação (Mestrado em Direito) – Faculdade de Direito da UFMG, Belo Horizonte, 2001, p. 37.
[53] GRECO, Rogério. **Curso de direito penal – parte geral**. 18 ed. rev. ampl. e atual. Rio de Janeiro: Impetus, 2016, p. 78.
[54] *Ibidem*, p. 78.

> *crime de perigo;* o *furto* em casa habitada absorve a *violação de domicílio;* o *homicídio* absorve a *lesão corporal* e o *porte de armas*; os "crimes do automóvel" absorvem a contravenção de "direção perigosa de veículo na via pública".
> É de notar-se ainda que a exclusão de uma norma por outra pode ocorrer mesmo no caso em que não haja unidade de fato ou um só contexto de ação. Um fato, embora configure crime, pode deixar de ser punível quando *anterior* ou *posterior* (*straglose Vor und Nachtat*) a outro crime mais grave, pressuposta a unidade de agente (...)[55]

Ademais, Vianna ensina que não se pode confundir crimes informáticos mediatos com as demais classificações. Para o autor, o delito informático mediato não se confunde com impróprio pois naquele há lesão ao bem jurídico informático, mesmo que tal pratica não seja penalizada devido a absorção. Por fim, expõe que diferentemente do que ocorre com os crimes informáticos mistos, aqui, há violação de dois tipos penais distintos.[56]

3.4 SUJEITOS DO CRIME

Assim como o conceito e a classificação dos crimes informáticos, saber quem são os sujeitos do crime é de suma importância. Os sujeitos do crime não dividido em sujeito ativo e passivo.

3.4.1 SUJEITO ATIVO

Tendo em vista que o crime pressupõe uma ação humana, somente o homem pode ser autor de crime, sendo **sujeito ativo** aquele que pratica fato descrito como crime, isto é, a pessoa que executa a figura descrita no tipo legal, segundo ensina Cezar Roberto Bitencourt:

> Por ser o crime uma *ação humana*, somente o ser vivo, nascido de mulher, pode ser autor de crime, embora em tempos remotos tenham sido condenados, como autores de crimes, animais, cadáveres e até estátuas. A *conduta* (ação ou omissão), pedra angular da Teoria do Crime, é produto exclusivo do Homem. A capacidade de ação, e de culpabilidade, exige a presença de uma *vontade*, entendida como *faculdade psíquica* da pessoa individual, que somente o ser humano pode ter.

---

[55] HUNGRIA, Nélson, FRAGOSO, Heleno Cláudio. **Comentários ao código penal,** v.1, tomo 1: arts. 1º ao 10º. 5 ed. Rio de Janeiro: Forense, 1976, p. 147/148.
[56] VIANNA, Túlio Lima. **Do acesso não autorizado a sistemas computacionais: fundamentos de direito penal informático.** 2001. 241 f. Dissertação (Mestrado em Direito) – Faculdade de Direito da UFMG, Belo Horizonte, 2001, p. 52.

> *Sujeito ativo* é quem pratica o fato descrito como crime na norma penal incriminadora. Para ser considerado sujeito ativo de um crime é preciso executar total ou parcialmente a figura descritiva de um crime. O Direito positivo tem utilizado uma variada terminologia para definir o sujeito ativo do crime, alterando segundo o diploma legal e, particularmente, segundo a fase procedimental. (...)[57]

Portanto, do mesmo modo que ocorre nos crimes comuns, o sujeito ativo do crime informático é aquele que pratica conduta ilícita atrás de um computador ou qualquer outro equipamento eletrônico ligado à rede (*internet*).

Em regra, o sujeito ativo dos crimes informáticos possui um nível intelectual maior em detrimento do seu conhecimento em informática, contudo, isso não significa que o autor da conduta deva ter conhecimento técnico. Essas condutas não são praticadas por leigos, guardando as suas devidas proporções, na medida em que nem todo crime informático exige "inteligência", como é o caso dos crimes contra a honra.

Nos crimes contra a honra, o crime pode ser consumado pela mera emissão de um e-mail, que não exige do agente um conhecimento aprofundado em informática.

Correntemente os sujeitos ativos dos crimes informáticos não conhecidos como *hackers*[58], contudo, essa terminologia está incorreta, haja vista referir-se aos especialistas em computador, sendo tal vocábulo criado pelo *Massachusetts Institute of Technology*. Esses especialistas de computador não possuem uma característica maliciosa [59], ou seja, *hackers* não são, em sua essência, criminosos.

A doutrina entende que seria correto utilizar o termo *"cracker"* para se referir ao sujeito ativo, eis que assim como o *hacker*, tem conhecimentos amplos de informática, contudo, os utiliza para o mal, ou seja, os utiliza para cometer crimes.

> O *hacker* atua através do "entrusismo", é um autodidata da informática, cujo objetivo se limita a vulnerar programas informáticos. Por outro lado, o *cracker,* igualmente detentor de uma curiosidade informática aguçada, não tem como objetivo apenas invadir programar ou ter acesso às informações, mas sim, adulterá-los.

---

[57] BITENCOURT, Cezar Roberto. **Tratado de direito penal: parte geral, 1.** 15. ed. rev. atual., ampl. São Paulo: Saraiva, 2010, p. 272.

[58] HACKER – Este indivíduo em geral domina a informática e é muito inteligente, adora invadir sites, mas na maioria das vezes não com a finalidade de cometer crimes, costumam se desafiar entre si, para ver que consegue invadir tal sistema ou página na internet, isto apenas para mostrar como estamos vulneráveis no mundo virtual. Várias empresas estão contratando há tempos os Hacker's para proteção de seus sistemas, banco de dados, seus segredos profissionais, fraudes eletrônicas, etc. (NOGUEIRA, Sandro D'Amato. **Crimes de informática.** São Paulo: BH Editora, 2008, p. 61.)

[59] COSTA, Fernando José da. ***Locus Delicti* nos crimes informáticos.** 2011. 355 f. Tese (Doutorado em Direito) – Faculdade de Direito da USP, São Paulo, 2011, p. 119.

> Estas denominações nem sempre vêm veiculadas de maneira correta pela mídia ou por pessoas que desconhecem a tecnicidade da linguagem adotada quando tratamos destes criminosos digitais. De qualquer maneira, estes criminosos da internet deixaram, há muito tempo, de ser apenas estudantes de computação querendo se destacar, mas tornaram-se agentes criminosos profissionais, organizados em máfias, que praticam golpes imensuráveis, com o auxílio das ferramentas tecnológicas cada vez mais evoluídas.[60]

Sobre isso, Marcos Flávio Araújo Assunção ensina o seguinte:

> Hacker White-Hat: Seria o "Hacker do bem", chamado de "hacker chapéu branco". É aquela pessoa que se destaca nas empresas e instituições por ter um conhecimento mais elevado que seus colegas, devido ao autodidatismo e à paixão pelo que faz. Não chega a invadir sistemas e causar estragos, exceto ao realizar testes de intrusão. Resumindo: tem um vasto conhecimento, mas não o usa de forma banal e irresponsável.
> Hacker Black-Hat: "Hacker do Mal" ou "chapéu negro". Esse, sim, usa seus conhecimentos para roubar senhas, documentos, causar danos ou mesmo realizar espionagem industrial. Geralmente tem seus alvos bem definidos e podem passar semanas antes de conseguir acesso onde deseja, se o sistema for bem protegido.[61]

Com efeito, atualmente, dizer que Hackers ou Cracker são sujeitos ativos dos crimes informáticos é um erro, tendo em vista que tais condutas podem ser praticadas por qualquer pessoa, independente do seu conhecimento informático.

3.4.2 SUJEITO PASSIVO

Ao titular do bem jurídico violado pela conduta criminosa dá-se o nome de sujeito passivo, que pode ser o ser humano, a pessoa jurídica ou Estado. O Estado sempre será sujeito passivo de todos os crimes.

Bitencourt esclarece que:

> Sujeito passivo é o titular do bem jurídico atingido pela conduta criminosa. Sujeito passivo do crime pode ser: o ser humano (ex.: crimes contra a pessoa); o Estado (ex.: crimes contra a Administração Pública); a coletividade (ex.: crimes contra a saúde pública); e, inclusive, pode ser a pessoa jurídica (ex.: crimes contra o patrimônio).
> Sob o aspecto formal, o Estado é sempre o sujeito passivo do crime, que poderíamos chamar de sujeito passivo mediato. Sob o aspecto material, sujeito passivo direto é o titular do bem ou interesse lesado. Nada impede, no entanto, que o próprio Estado seja o sujeito passivo imediato, direto, como ocorre quando o Estado é o titular do interesse jurídico lesado, como, por

---

[60] CONTE, Christiany Pegorari. **Jurisdição e competência nos crimes informáticos.** Revista Brasileira de Meio Ambiente Digital e Sociedade da Informação. V. 01, nº. 01, p. 49-208, 2014, p. 117.
[61] ASSUNÇÃO, Marco Flávio Araújo. **Segredos do Hacker Ético.** 2ª ed. Visual Books: Florianópolis, 2008, p. 13.

> exemplo, segundo a doutrina majoritária, nos crimes contra a Administração Pública.[62]

No mesmo sentido, Cleber Masson ensina o seguinte:

> É o titular do bem jurídico protegido pela lei penal violada por meio de conduta criminosa. Pode ser denominada de **vítima** ou de **ofendido**, e divide-se em duas espécies:
> **1) Sujeito passivo constante, mediato, formal, geral, genérico ou indireto**: é o Estado, pois a ele pertence o direito público subjetivo de exigir o cumprimento da legislação penal.
> (...)
> **2) Sujeito passivo eventual, imediato, material, particular, acidental ou direto:** é o titular do bem jurídico especificamente tutelado pela lei penal. Exemplo: o proprietário do carro subtraído no crime de furto.
> O Estado sempre figura como sujeito passivo constante. Além disso, pode ser sujeito passivo eventual, tal como ocorre nos crimes contra a Administração Pública.
> A pessoa jurídica pode ser vítima de diversos delitos, desde que compatíveis como a sua natureza.[63]

No início as vítimas dos crimes informáticos eram em sua maioria pessoas jurídicas, não obstante, pelo que se viu até aqui, assim como qualquer pessoa pode praticar tais crimes, qualquer pessoa pode ter seu bem jurídico prejudicado.

3.5 DELITOS INFORMÁTICOS EM ESPÉCIE

Nesse subcapítulo far-se-á a análise de alguns crimes informáticos impróprios, os mais corriqueiros, contudo, não será realizado um estudo aprofundado dos temas, mas de que forma tais crimes podem ocorrer.

3.5.1 CRIMES CONTRA A PESSOA

Dentre os vários bens jurídicos resguardados pelo Direito Penal, o Legislador preocupou-se inicialmente com a tutela dos crimes contra a pessoa. A legislação penal, na parte especial, dividiu os bens jurídicos tutelados em 11 títulos, quais sejam: Título I – Dos crimes contra a pessoa; Título II – Dos crimes contra o patrimônio; Título III – Dos crimes contra a propriedade imaterial. Título IV – Dos crimes contra a

---

[62] BITENCOURT, Cezar Roberto. **Tratado de direito penal: parte geral, 1.** 15. ed. rev. atual., ampl. São Paulo: Saraiva, 2010, p. 273.
[63] MASSON, Cleber Rogério. **Direito penal esquematizado – parte geral – vol. 1.** 4ª. ed. rev., atual. e ampl. São Paulo: Método, 2011, p. 182/183.

organização do trabalho; Título V – Dos crimes contra o sentimento religioso e o respeito aos mortos; Título VI – Crimes contra a dignidade sexual; Título VII – Dos crimes contra a família; Título VIII – Dos crimes contra a incolumidade pública; Título IX – Dos crimes contra a paz pública; Título X – Dos crimes contra a fé pública e; Título XI – Dos crimes contra a Administração Pública.

Com efeito, nessa primeira parte será realizada a análise de alguns dos crimes previstos no Título I, que trata dos crimes contra a pessoa, que são divididos nos seguintes capítulos: I — Dos crimes contra a vida (arts. 121 a 128); II — Das lesões corporais (art. 129); III — Da periclitação da vida e da saúde (arts. 130 a 136); IV — Da rixa (art. 137); V — Dos crimes contra a honra (arts. 138 a 145); VI — Dos crimes contra a liberdade individual (arts. 146 a 154), que, por sua vez, subdivide-se em quatro seções: Dos crimes contra a liberdade pessoal (arts. 146 a 149); Dos crimes contra a inviolabilidade do domicílio (art. 150); Dos crimes contra a inviolabilidade de correspondência (arts. 151 e 152); Dos crimes contra a inviolabilidade dos segredos (arts. 153 e 154).

3.5.1.1 HOMICÍDIO

O homicídio, senão o pior, é uma das mais inescrupulosas ações praticadas pelos seres humanos, pois consiste no ato de “Matar alguém”, cujo tipo legal está previsto no artigo 121 do Código Penal.

Nesse sentido, entenderam Nelson Hungria e Heleno Cláudio Fragoso:

> O homicídio e o tipo central dos crimes contra a Vida e é o ponto culminante na orografia dos crimes. É o *crime* por excelência. E o padrão da delinquência *violenta* ou *sanguinária,* que representa como que uma reversão atávica as eras primevas, em que a luta pela vida, presumivelmente, se operava com o uso normal dos meios brutais e animalescos. E a mais chocante violação do senso moral médio da humanidade civilizada.[64]

O núcleo do tipo penal do Homicídio é verbo matar, que consiste na supressão da vida de alguém (elemento objetivo). Apesar da vida ser um bem do indivíduo, que se manifesta como direito fundamento segundo o ordenamento jurídico vigente, é

[64] HUNGRIA, Nélson, FRAGOSO, Heleno Cláudio. **Comentários ao código penal,** v.5, arts. 121 ao 136. 5 ed. Rio de Janeiro: Forense, 1979, p. 25.

interesse também do Estado o seu resguardo, justamente por conta dessa fundamentalidade.

Cezar Roberto Bitencourt preleciona que:

> Homicídio e a eliminação da vida de alguém levada a efeito por outrem. Embora a vida seja um bem fundamental do ser individuai-social, que é o homem, sua proteção legal constitui um interesse compartido do indivíduo e do Estado. A importância do bem vida justifica a preocupação do legislador brasileiro, que não se limitou a protege-la com a tipificação do homicídio, em graus diversos (simples, privilegiado e qualificado), mas lhe reservou outras figuras delituosas, como o aborto, o suicídio e o infanticídio, que, apesar de serem figuras autônomas, não passam de extensões ou particularidades daquela figura central, que pune a supressão da vida de alguém.[65]

É sabido que o sujeito ativo pode ser qualquer pessoa, assim como o sujeito passivo, isto é, qualquer pessoa pode praticar, bem como ser vítima do crime, haja vista tratar-se de delito comum, consoante expõe de Rogério Greco:

> Sujeito ativo do delito de homicídio pode ser qualquer pessoa, haja vista tratar-se de um delito comum, uma vez que o tipo penal não delimita sua prática por determinado grupo de pessoas que possua alguma qualidade especial. Sujeito passivo, da mesma forma, também pode ser qualquer pessoa, em face da ausência de qualquer especificidade constante do tipo penal. É, portanto, o ser vivo, nascido de mulher.
> O importante é que matar alguém seja entendido como a morte de um homem, produzida por outro homem, afastando-se, portanto, por absurdo e atípico, o folclore que se escuta no meio forense de casos em que já houve denúncia em face de alguém que provocou a morte de uma vaca, um cachorro, etc.[66]

Outrossim, em que pese o sujeito passivo possa ser qualquer pessoa, caso seja mulher e o crime tenha ocorrido por motivo de sexo feminino (violência doméstica e família e menosprezo ou discriminação à condição de mulher), o delito não será o de homicídio, mas de feminicídio, cuja pena é bem superior à conduta comum, conforme se verifica na redação do disposto legal, que passou a viger no dia 09 de março de 2015, através da Lei nº. 13.104/2015:

> **Feminicídio**
> VI - contra a mulher por razões da condição de sexo feminino:
> VII – contra autoridade ou agente descrito nos arts. 142 e 144 da Constituição Federal, integrantes do sistema prisional e da Força Nacional de Segurança

---

[65] BITENCOURT, Cezar Roberto. **Tratado de direito penal: parte especial, 2.** 10. ed. São Paulo: Saraiva, 2010, p. 45.
[66] GRECO, Rogério. **Curso de direito penal – parte especial, volume II: introdução à teoria geral da parte especial: crimes contra a pessoa**. 11 ed. rev. e atual. Rio de Janeiro: Impetus, 2015, p. 134.

> Pública, no exercício da função ou em decorrência dela, ou contra seu cônjuge, companheiro ou parente consanguíneo até terceiro grau, em razão dessa condição:
> Pena - reclusão, de doze a trinta anos.
> § 2º-A Considera-se que há razões de condição de sexo feminino quando o crime envolve:
> I - violência doméstica e familiar;
> II - menosprezo ou discriminação à condição de mulher.

Pois bem, é impressionante saber que homicídios podem ser praticados com a utilização de um aparelho eletrônico ligado à internet, em que pese, na maioria das vezes, a internet não é a causadora direta do mal.

O atentando terrorista ocorrido no dia 11 de setembro de 2001 contra os Estados Unidos da América, que destruiu o edifício *World Trade Center*, bem como causou danos no Pentágono, é uma demonstração clara do que a internet pode provocar quando utilizada com fins ilícitos.[67]

Com efeito, o ataque foi provocado pela organização fundamentalista islâmica al-Qaeda, que com a utilização de dezenove terroristas, sequestraram quatro aviões. Os criminosos conseguiram derrubar três aviões, sendo dois nas torres gêmeas e um no Pentágono, provocando a morte de aproximadamente três mil pessoas. O quarto avião não caiu porque os passageiros conseguiram render os terroristas.[68]

Enfim, esse absurdo acontecimento só foi possível devido aos benefícios que a internet propiciou, pois ela garantiu que os terroristas se comunicassem, comprassem as passagens, bem como obtivessem todas as informações necessários para consumar seus anseios.[69]

Mas não é só, outras condutas podem ser praticadas para causar matar, por exemplo, a internet pode ser utilizada para ativar bombas ou qualquer outro aparelho que coloque risco à vida.

O Poder Legislativo até buscou criminalizar, legalmente, condutas informáticas que atentassem contra a vida no Projeto de Lei 76/2000, que dispunha no artigo 1º, §4º, o seguinte:

---

[67] COSTA, Fernando José da. ***Locus Delicti* nos crimes informáticos.** 2011. 355 f. Tese (Doutorado em Direito) – Faculdade de Direito da USP, São Paulo, 2011, p. 89.
[68] SANT'ANNA, Ivan. **Plano de Ataque: a história dos vôos de 11 de setembro.** Rio de Janeiro: Objetiva, 2006.
[69] COSTA, Fernando José da. ***Locus Delicti* nos crimes informáticos.** 2011. 355 f. Tese (Doutorado em Direito) – Faculdade de Direito da USP, São Paulo, 2011, p. 89.

> Art. 1º Constitui crime de uso indevido da informática:
> (...)
> § 4º contra a vida e integridade física das pessoas:
> I – o uso de mecanismos da informática para ativação de artefatos explosivos, causando danos, lesões ou homicídios;
> II – a elaboração de sistema de computador vinculado a equipamento mecânico, constituindo-se em artefatos explosivos.
> Pena: reclusão, de um a seis anos e multa.

Não obstante, o respectivo projeto foi arquivado e substituído pelo Projeto de Lei Complementar 89/2003, que não fez menção às respectivas condutas, talvez pela possibilidade de conflito de normas ou pela eventual desnecessidade do tipo legal, em razão da tutela pelo Direito Penal.

É possível verificar uma clara contrariedade de posicionamentos do Poder Legislativo quando promulgam leis que regulamentam crimes. Ora, promulgaram o tipo penal do feminicídio, que é totalmente desnecessário em razão da existência do homicídio, mas deixaram de tratar condutas informáticas que causam a morte.

Não há na legislação penal nenhum tipo penal que criminalize ou que agrave a pena de atos que provoquem lesões ou homicídios, mediante a utilização de sistemas ou aparelhos informáticos.

3.5.1.2 INDUZIMENTO, INSTIGAÇÃO OU AUXILIO A SUICÍDIO

Suicídio consiste na “eliminação voluntária e direta da própria vida. Para que haja suicídio, é imprescindível a intenção positiva de despedir-se da vida”[70], cujo tipo penal dispõe o seguinte:

> 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.
> Parágrafo único - A pena é duplicada:
> Aumento de pena
> I - se o crime é praticado por motivo egoístico;
> II - se a vítima é menor ou tem diminuída, por qualquer causa, a capacidade de resistência.

[70] HUNGRIA, Nélson, FRAGOSO, Heleno Cláudio. **Comentários ao código penal,** v.5, arts. 121 ao 136. 5 ed. Rio de Janeiro: Forense, 1979, p. 231.

Registra-se que praticar suicídio não é crime, embora seja uma conduta antijurídica, tendo em vista que o ordenamento jurídico protege a vida, que é um bem público indisponível, ou seja, mesmo não havendo responsabilização penal àquele que tenta praticado suicídio, a legislação brasileira não outorga o direito de dispor da própria vida, conforme expõe Fernando Capez:

> O suicídio é a deliberada destruição da própria vida. Suicida, segundo o Direito, é somente aquele que busca direta e voluntariamente a própria morte. Apesar de o suicídio não ser um ilícito penal, é um fato antijurídico, dado que a vida é um bem público indisponível, sendo certo que o art. 146, § 3º, II, do Código Penal prevê a possibilidade de se exercer coação contra quem tenta suicidar-se, justamente pelo fato de que a ninguém é dado o direito de dispor da própria vida. Não obstante a lei penal não punir o suicídio, cujas razões de índole político-criminal veremos logo mais adiante, ela pune o comportamento de quem induz, instiga ou auxilia outrem a suicidar-se. É que, sendo a vida um bem público indisponível, o ordenamento jurídico veda qualquer forma de auxílio à eliminação da vida humana, ainda que esteja presente o consentimento do ofendido.[71]

Ademais, segundo ensina Nélson Hungria, o crime só será punido se a conduta do agente se consumar ou causar lesões corporais. Eis o que dispõe o professor:

> (...). É o que acontece com o crime de participação em suicídio: embora o crime se apresente consumado com o simples induzimento, instigação ou prestação de auxilio, a punição está condicionada à superveniente *consumação* do suicídio ou, no caso de mera tentativa, à produção de *lesão corporal de natureza grave* na pessoa do frustrado desertor da vida. Se não se segue, sequer, a tentativa, ou esta não produz lesão alguma ou apenas ocasione uma lesão de natureza leve, a participação ficará impune.[72]

Por conta disso, só pratica o crime aquele que induz, instiga ou auxilia o cometimento do suicídio. Induzir é sugerir, suscitar, inspirar que alguém tire a própria vida. Instigar significa fomentar ou reforçar o desejo pelo suicídio. Por fim, auxiliar consiste na ajuda material/concreta, que pode ocorre antes ou durante o suicídio.

Conforme Rogério Sanches Cunha:

> a) *induzimento:* hipótese em que o agente faz nascer na vítima a ideia e a vontade mórbida. Aqui o sujeito passivo nem sequer cogitava de eliminar a própria vida, sendo convencido pela ação do agente;

---

[71] CAPEZ, Fernando. **Curso de direito penal, volume 2, parte especial – dos crimes contra a pessoa e dos crimes contra o sentimento religioso e contra o respeito aos mortos (arts. 121 a 212)**. 10. ed. São Paulo: Saraiva, 2010, p. 120.

[72] HUNGRIA, Nélson, FRAGOSO, Heleno Cláudio. **Comentários ao código penal,** v.5, arts. 121 ao 136. 5 ed. Rio de Janeiro: Forense, 1979, p. 235.

> b) *instigação:* caso em que o autor reforça a vontade mórbida preexistente na vítima. Aqui o sujeito passivo já pensava em se suicidar, sendo tal propósito reforçado pelo agente;
> c) *auxílio:* prestando o agente efetiva assistência material, facilitando a execução do suicídio, quer fornecendo, quer colocando à disposição do ofendido os meios necessários para fazê-lo (ex.: emprestando instrumentos letais).[73]

Diante do exposto, não é muito difícil imaginar que o respectivo crime pode ser praticado através da internet. Exemplificando, o médico estadunidense Jack Kevorkian, conhecido como Doutor da Morte, falecido em 2011, confessou que havia contribuído com a prática de 130 suicídios, vários deles através da internet, isto é, o médico utilizava a internet para auxiliar pacientes em estado terminal a cometerem suicídio.

Destaca-se que diversos suicídios já foram cometidos no Brasil com o auxílio da internet.

A Revista Época, por exemplo, publicou uma matéria aduzindo que o suicídio do adolescente Vinícius Gageiro Marques, que possuía apenas 16 anos de idade, seria o primeiro "suicídio.com" ocorrido no país. Yoñlu, como era conhecido também, cometeu suicídio no dia 26 de julho de 2006, por volta das 15h30min. O jovem tinha problemas psicológicos e decidiu cometer suicídio e para tanto pediu auxílio aos internautas num grupo de discussão. A morte ocorreu por asfixia, devido a inalação de monóxido de carbono, emitidos pela queima de carvão dentro do banheiro de sua residência.[74]

Ademais, ainda em 2006, na cidade de Ponta Grossa/PR, o estudante Thiago Arruda cometeu suicídio após sofrer inúmeras ofensas, que lhe foram dirigidas pela rede social Orkut. Os ataques caluniosos, difamatórios e injuriosos lhe causaram sofrimento psicológico – sendo chamado de homossexual e pedófilo – ao ponto de manifestar o desejo de cometer suicídio, caso os ataques não cessassem.[75]

---

[73] CUNHA, Rogério Sanches. **Manual de direito penal – parte especial (arts. 121 ao 361).** 8 ed. rev. ampl. e atual. Salvador/BA: JusPODIVM, 2016, p. 82.
[74] BRUM, Eliane; AZEVEDO, Solange. **Suicídio.com – Sites na internet incentivam adolescentes como o gaúcho Yoñlu a se matar e ajudam a escolher o método**. Disponível em: http://revistaepoca.globo.com/Revista/Epoca/0,,EDR81603-6014,00.html, Acesso em: 20 de set. 2016.
[75] OLIVEIRA, Diego Bianchi de; SILVA, Ricardo Guilherme Silveira Corrêa. **O viés digital do suicídio: instigação, induzimento e auxílio ao suicídio em ambientes virtuais.** In: XXIV CONGRESSO NACIONAL DO CONPEDI – UFMG/FUMEC/Dom Helder Câmara, 2015, Florianópolis, Direito Penal e Constituição, Florianópolis/MG, 2015, p. 563-581, p. 576.

Ressalta-se que as agressões não pararam e os incentivos e orientações ao suicídio começaram. Thiago “colocou uma mangueira no cano do escape do carro, entrou no veículo, ligou o motor e morreu ao inalar o monóxido de carbono”[76] emitido pelo veículo.

É possível verificar, portanto, que a velocidade de tráfego das informações e a suposta impossibilidade de identificação do infrator, torna fácil e interessante para o cometimento de inúmeros crimes, por isso é fundamental a cooperação internacional nessa área, bem como o desenvolvimento das tecnologias para coibição de crimes.

3.5.1.3 DOS CRIMES CONTRA A HONRA

A Constituição Federal consigna que a honra é um bem jurídico inviolável, garantindo ao prejudicado reparação pelos danos materiais e morais que sofrer, conforme estabelece o artigo 5º, inciso X:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> (...)
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

A honra se constrói com o tempo, durante a vida das pessoas[77], tornando-as merecedoras de respeito.

Cleber Masson expõe que:

> Honra é o conjunto de qualidades físicas, morais e intelectuais de um ser humano, que o fazem merecedor de respeito no meio social e promovem sua autoestima. É um sentimento natural, inerente a todo homem e cuja ofensa produz uma dor psíquica, um abalo moral, acompanhados de atos de repulsão ao ofensor. Representa o valor social do indivíduo, pois está ligada à sua aceitação ou aversão dentro de um dos círculos sociais em que vive, integrando seu patrimônio. Um patrimônio moral que merece proteção.
> Cuida-se de direito fundamental do homem, previsto no art. 5.°, inciso X, da Constituição Federal. Esse é o fundamento constitucional dos crimes contra a honra, em consonância com uma análise constitucionalista do Direito Penal.

---

[76] FABEL, Evandro. **Polícia Civil investiga possível incentivo ao suicídio no Orkut.** Disponível em: http://www.gazetadigital.com.br/conteudo/show/secao/4/materia/138370. Acesso em: 20 de set. 2016.
[77] GRECO, Rogério. **Curso de direito penal – parte especial, volume II: introdução à teoria geral da parte especial: crimes contra a pessoa**. 11 ed. rev. e atual. Rio de Janeiro: Impetus, 2015, p. 415.

> Com efeito, toda lei penal incriminadora somente se legitima quando tutela um bem jurídico consagrado pela Constituição Federal.[78]

Nada obstante, para melhor interpretação, a honra foi dividida em objetiva e subjetiva. A primeira se refere a reputação do indivíduo, isto é, trata da imagem que a sociedade possui de determinada pessoa. Já honra subjetiva diz respeito aos sentimentos pessoais de cada pessoa, ou seja, é o juízo que cada pessoa faz de si mesmo.[79]

Com efeito, essa diferenciação é fundamental para identificar o momento consumativo de cada infração contra a honra definida pelo código penal, quais sejam: calúnia, difamação e injúria.

Eis o que dispõem os tipos legais:

> Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime:
> Pena - detenção, de seis meses a dois anos, e multa.
> § 1º - Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga.
> § 2º - É punível a calúnia contra os mortos.
> (...)
> Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação:
> Pena - detenção, de três meses a um ano, e multa.
> (...)
> Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:
> Pena - detenção, de um a seis meses, ou multa.

O delito do artigo 138, a calúnia, é o crime mais grave dentre os crimes contra a honra. Caluniar representa a conduta de imputar a alguém, de maneira falsa, conduta definida como crime, ou seja, é o ato de conferir a alguém a incumbência da prática de um crime, que pode não ter ocorrido ou até mesmo que não foi praticado pelo sujeito passivo.[80]

Rogério Greco expõe que o tipo penal possui três características principais:

> a) a imputação de um *fato*;
> b) esse fato imputado à vítima deve, obrigatoriamente, ser *falso*;

---

[78] MASSON, Cleber. **Direito penal esquematizado: parte especial – vol. 2**. 7ª. ed. rev., atual. e ampl. Rio de Janeiro: Forense; São Paulo: MÉTODO, 2015, p. 174/175.
[79] CUNHA, Rogério Sanches. **Manual de direito penal – parte especial (arts. 121 ao 361).** 8 ed. rev. ampl. e atual. Salvador/BA: JusPODIVM, 2016, p. 173.
[80] CAPEZ, Fernando. **Curso de direito penal, volume 2, parte especial – dos crimes contra a pessoa e dos crimes contra o sentimento religioso e contra o respeito aos mortos (arts. 121 a 212)**. 10. ed. São Paulo: Saraiva, 2010, p. 279.

c) além de falso, o fato deve ser definido como *crime*.[81]

Com efeito, o bem jurídico protegido pelo crime é a honra objetiva, ou seja, a reputação do indivíduo perante à sociedade.

A difamação, por sua vez, prevista no artigo 139 do Código Penal, se refere a conduta de ofender, publicamente, a reputação de uma pessoa, violando, assim como na calúnia, a honra objetiva da vítima.

Importante ressaltar que a ofensa não precisa ser verdadeira ou falsa, tampouco definida como crime, já que isso foi reservado à calúnia, basta que macule a reputação da vítima.

Nesse sentido, Guilherme de Souza Nucci, analisando o núcleo do tipo do crime de difamação, consigna o seguinte:

> (...) difamar significa desacreditar publicamente uma pessoa, maculando-lhe a reputação. Nesse caso, mais uma vez, o tipo penal foi propositalmente repetitivo. Difamar já significa imputar algo desairoso a outrem, embora a descrição abstrata feita pelo legislador tenha deixado claro que, no contexto do crime do art. 139, não se trata de qualquer fato inconveniente ou negativo, mas sim fato ofensivo à sua reputação. Com isso, exclui os fatos definidos como crime – que ficaram para o tipo penal da calúnia – bem como afastou qualquer vinculação à falsidade ou veracidade dos mesmos. Assim, difamar uma pessoa implica em divulgar fatos infamantes à sua honra objetivo, sejam eles verdadeiros ou falsos.[82]

Por fim, tem-se o delito de injuria, que ao contrário dos crimes anteriores, fere a honra subjetiva da vítima, isto é, viola o sentimento que ela tem de si mesmo; seus atributos morais, intelectuais ou físicos.

Em outras palavras, Nelson Hungria disciplinou que injúria:

> É a manifestação, por qualquer meio, de um conceito ou pensamento que importe ultraje, menoscabo ou vilipêndio contra alguém. O bem jurídico lesado pela injúria é, prevalentemente, a chamada *honra subjetiva*, isto é, o sentimento da própria honorabilidade ou respeitabilidade pessoal. Se na calúnia ou na difamação o agente visa, principalmente, ao descrédito moral do ofendido perante terceiro, na injúria seu objetivo primacial é feri-lo no seu brio ou pudor. (...) Traduz uma opinião pessoal do agente, desacompanhada da menção de fatos concretos ou precisos. É a palavra insultuosa, o epíteto

[81] GRECO, Rogério. **Curso de direito penal – parte especial, volume II: introdução à teoria geral da parte especial: crimes contra a pessoa**. 11 ed. rev. e atual. Rio de Janeiro: Impetus, 2015, p. 421.
[82] NUCCI, Guilherme de Souza. **Código penal comentado**. 10. ed. rev., atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2010, p. 679.

> aviltante, o *xingamento*, o impropério, o gesto ultrajante, todo e qualquer ato, enfim, que exprima desprezo, escárneo, ludíbrio.[83]

Diante dos conceitos apresentados, é possível observar que é plenamente viável a práticas dos crimes contra a honra através de meios eletrônicos ligados à *internet.* Esses delitos podem ser praticados com auxílio das redes sociais (Twitter, Facebook, Instagram, Snapchat) por e-mail, Skype, jornais digitais, bem como outra rede privada ou pública de comunicação digital.

Atualmente, é muito fácil ofender a honra objetiva ou subjetiva de alguém, ante os sistemas informáticos existentes e tais condutas estão sendo reconhecidas pelos Tribunais de Justiça do país.

Exemplificando, veja-se a jurisprudência abaixo, que trata de agressões perpetradas em desfavor do ex-presidente da república Fernando Henrique Cardoso:

> PENAL - APELAÇÃO CRIMINAL - INJÚRIA EM "SALA DE BATE-PAPO" NA INTERNET - AGRESSÕES À DIGNIDADE E DECORO DO PRESIDENTE DA REPÚBLICA -CONTEÚDO PÚBLICO DO SITE - AFASTADA A ALEGAÇÃO DE NULIDADE POR AUSÊNCIA DE AUTORIZAÇÃO JUDICIAL PARA CONHECIMENTO DO TEOR DA CONVERSA - DIÁLOGO PÚBLICO - O ANONIMATO NÃO É PROTEGIDO JURIDICAMENTE - DETERMINAÇÃO JUDICIAL EXISTENTE 'AD CAUTELAM' APENAS PARA IDENTIFICAÇÃO DO OFENSOR - CRIME QUE PROTEGE A HONRA SUBJETIVA - CONSUMAÇÃO NO MOMENTO EM QUE A VÍTIMA TOMA CIÊNCIA DO TEOR DO DIÁLOGO ULTRAJANTE - "ANIMUS INJURIANDI" EXPLÍCITO E INEQUÍOVOCO - CONDENAÇÃO MANTIDA - RECURSO DESPROVIDO. 1. Apelação criminal contra a sentença proferida em ação penal destinada a apurar a prática dos crimes descritos nos artigos 138, 139, 140 c/c 141, I do Código Penal, na qual foi condenado por injúria contra o Sr. Fernando Henrique Cardoso, então Presidente da República. 2. Consta da denúncia que o réu, no dia 05/11/2001, em São Paulo, por meio da rede mundial de computadores, INTERNET, imputou ao Presidente da República do Brasil daquela época a prática dos crimes de corrupção ativa e de responsabilidade, além de fatos ofensivos à sua reputação, bem como ofendeu a dignidade e decoro da referida autoridade. Nos termos da inicial o denunciado foi identificado como signatário do login jfbadvoc@ig.com.br por meio do qual foram "assacadas" as expressões ofensivas à honra e à reputação do Sr. Fernando Henrique Cardoso. Ainda segundo a exordial, o próprio réu teria confirmado ser o responsável pela mensagem lançada no site "democacia.com.br", que deu ensejo à presente ação penal pública, sob as escusas de que não teria passado de um ato de molecagem. 3 A vítima sentiu-se ofendida com as declarações veiculadas por vontade do denunciado e pediu a responsabilização do mesmo o mais rápido possível. Assim, representou ao Sr. Ministro da Justiça, o qual requisitou ao Ministério Público Federal que deflagrasse esta ação penal. 4. A injúria que ensejou a condenação consumou-se no dia 02/02/2002, data em que a vítima encaminhou uma carta ao Sr. Ministro da Justiça relatando o ocorrido e pedindo as providências cabíveis para responsabilização penal do ofensor. A

[83] HUNGRIA, Nélson, FRAGOSO, Heleno Cláudio. **Comentários ao código penal,** v.6, arts. 137 ao 154. 5 ed. Rio de Janeiro: Forense, 1980, p. 90/91.

denúncia foi recebida em 22/04/2003 e a sentença condenatória publicada em 01/04/2005. 5. A ação penal inicialmente teve curso na 12ª Vara Federal do Distrito Federal, que declinou da competência, quando se identificou a origem da mensagem que maculou a honra presidencial, de tal sorte que prosseguiu na 1ª Vara Federal em São Paulo. 6. O Parquet Federal, após análise de folhas de antecedentes, propôs a suspensão condicional do processo, que não foi aceita pelo réu. 7. O apelante foi absolvido das imputações de difamação e calúnia e condenado ao cumprimento de 1 (um) mês de detenção, em regime inicial aberto e 13 (treze) dias-multa no valor unitário de 1/10 (um décimo) do salário mínimo vigente ao tempo do crime, a ser atualizado na execução, pelo crime de injúria. A pena privativa de liberdade foi substituída por 1 (uma) restritiva de direito consistente ao pagamento de 1 (um) salário mínimo, que o réu deverá pagar a uma entidade pública ou privada com destinação social cadastrada no Juízo das Execuções Penais. 8. Esclarece-se que qualquer pessoa poderia participar dos debates ultrajantes, bastando para tanto se cadastrar no site www.democracia.com.br , informando nome, e-mail, cidade e estado. Não houve dificuldade em se obter o conteúdo do diálogo insultoso, porque o acesso ao site era, de fato, livre. O obstáculo encontrado durante as investigações foi o de se identificar a autoria das ofensas proferidas contra o então Presidente Fernando Henrique Cardoso. Para tanto, houve determinação judicial. 9. Não há de se falar em nulidade, pois embora não haja proteção legal aos usuários de e-mails, 'ad cautelam', com fulcro na legislação pertinente ao sigilo de dados, houve intervenção judicial para se apurar a autoria delituosa, sendo certo que o diálogo ultrajante sob o tema "FHC é um canalha" já era público. Não havia dado sigiloso protegido a justificar a necessidade de uma ordem judicial. Precedente do STJ. 10. A autoria é inconteste, pois foi admitida pelo réu em seu interrogatório na fase investigatória bem como em juízo. A tese defensiva é a de que o réu "não sabia" que sua conversa, numa sala de bate-papo da Internet, poderia ser acessada livremente por outras pessoas. Aduz que pensava tratar-se de um colóquio reservado, privado. Entretanto, tal argumento é patético e supõe ingenuidade dos julgadores. Não tem qualquer valia para escusar o réu do crime de injúria, pois referido tipo penal incriminador não visa proteger a honra objetiva do ofendido, mas a sua honra subjetiva 11. A discussão acerca da divulgação e publicidade do teor da conversa em tese poderia até ter importância no caso da calúnia e difamação, que têm por objetividade jurídica a reputação e a boa fama que o ofendido goza perante a sociedade. Porém no caso da injúria, ora em análise, a exposição a terceiros dos fatos ofensivos é irrelevante, porque o que se pretende preservar é o sentimento pessoal que cada um dos indivíduos possui acerca de seus atributos físicos, intelectuais e morais. 10. Mesmo que o réu pensasse ter um único receptor dos comentários altamente agressivos à honra do Presidente, seria perfeitamente possível que este o levasse ao conhecimento de Fernando Henrique Cardoso. A previsibilidade deste resultado configura dolo eventual. Para a consumação do delito, prescinde-se que as ofensas sejam deferidas diretamente à vítima, conforme remansosa jurisprudência. 11. É inegável que expressões como "narcisista safado, falcatruador, histriônico, pústula, ordinário, corrupto e homúnculo" afetam tanto a honra-dignidade quanto a honra-decoro de qualquer homem. O apelante manifesta, inclusive, a vontade de "vomitar" cada vez que ouve o nome do ofendido e de mandá-lo "de volta ao esgoto", sendo explícito e inequívoco o dolo específico. 12. Os comentários que levaram à denúncia do apelante não podem ser tratados como se fossem informativos ou uma crítica séria e objetiva à política governamental. Do seu teor se extrai a deliberada intenção de enxovalhar e aviltar de forma absolutamente visceral o nome do então Presidente da República. A carga negativa das expressões injuriosas "per si" evidencia o "animus injuriandi". Mormente porque o ofensor é advogado, sexagenário e se expressa com vocabulário de considerável erudição. 13. As matérias jornalísticas acostadas aos autos são irrelevantes porque não se avalia in casu a reputação de Fernando Henrique Cardoso e

> tampouco a veracidade das práticas imorais e criminosas que o réu lhe atribuiu. 14. Mantida na íntegra a sentença condenatória pelo crime de injúria. (TRF-3 - ACR: 1855 SP 2003.61.81.001855-1, Relator: DESEMBARGADOR FEDERAL JOHONSOM DI SALVO, Data de Julgamento: 06/03/2007, PRIMEIRA TURMA,)

No julgamento acima, o sujeito ativo enviou para um site mensagens injuriosas, que ofendiam a reputação, a dignidade e o decoro de Fernando Henrique Cardoso, Ex-Presidente da República. O autor do crime ofendeu a honra subjetivo da vítima ao chamá-lo de narcisista, safado, falcatruador, histriônico (histérico), pústula (depravado), ordinário, corrupto e homúnculo (insignificante).

Com efeito, como consta no acórdão, o *"animus injuriandi"*, ou seja, a intenção de injuriar, restou devidamente demonstrada quando o condenado manifestou vontade de vomitar toda vez que houve o nome da vítima, bem como pelo fato de sentir vontade de manda-lo de volta para o esgoto.

Ademais, é possível observar ainda que a autoridade policial encontrou dificuldade em identificar o criminoso, pois como a ofensa foi praticada pela internet, a única informação que se tinha era o *login* de acesso do sujeito, que só foi localizado quando o site forneceu as informações cadastrais do usuário, cuja ordem foi determinada pela justiça.

Desse modo, é possível observar a dificuldade enfrentada pela autoridade policial em identificar os autores de crimes informáticos, que utilizam o meio digital para se ocultarem. Por conta disso, é essencial que as polícias estejam bem preparadas e o Poder Judiciário atento à nova realidade de forma que utilize os meios legais que estão ao seu alcance para contribuir na localização dos sujeitos que estão atrás das telas dos equipamentos eletrônicos.

3.5.2 DOS CRIMES CONTRA O PATRIMÔNIO

A parte que tutela os crimes contra o patrimônio é dividia em oito capítulos: Capítulo I – Do furto (arts. 155 e 156), Capítulo II – Do roubo e da extorsão (arts. 157 a 160), Capítulo III – Da usurpação (arts. 161 a 162), Capítulo IV – Do dano (arts. 163 a 167), Capítulo V – Da apropriação indébita (arts. 168 a 170), Capítulo VI – Do estelionato (arts. 171 a 179); Capítulo VII – Da receptação (art. 180); Capítulo VIII – Disposições gerais (arts. 181 a 183).

Entre os vários crimes contra o patrimônio previstos no Código Penal, tratar-se-á aqui somente do furto e do estelionato, previstos no artigo 155 e 171, respectivamente.

Pode-se dizer que a internet facilitou a vida dos criminosos, que não precisam sair da frende de seus computadores para se arriscarem na rua, isto é, aqueles que não tinham coragem suficiente para cometer crimes, por terem medo de serem preso em flagrante e processados, encontraram na internet um meio simplificado para obter vantagens.

Nesse sentido, Costa pontua que:

> Com a internet as pessoas que antes não tinham coragem de subtrair o patrimônio alheio, com a oportunidade de, sem sair da frente de um computador ou de correr o risco de ser surpreendida no instante da obtenção da vantagem, passaram a praticar este delito, quer motivadas pelo interesse econômico, quer motivadas pela vaidade atrelada à superação de barreiras de segurança informática ou ainda pela improvável possibilidade de serem presas em flagrante ou até condenadas.[84]

Todos os dias pessoas utilizam a internet para fins comerciais, fazendo compras e transferindo de valores, e para isso deixam seus dados pessoais à disposição de empresas, que se não possuírem um excelente sistema de segurança digital, facilitarão a atuação dos bandidos, conhecidos como "*Hacker Black-Hat"* ou "*Cracker".*

3.5.2.1 DO FURTO

O crime de furto, previsto no artigo 155 do Código Penal, representa o ato de subtrair para si ou para outrem coisa alheia móvel, cuja ação ocorre sem a utilização de violência.

Com efeito, furto "significa apoderar-se ou assenhorear-se de coisa pertencente a outrem, ou seja, torar-se senhor ou dono daquilo que, juridicamente, não lhe pertence."[85]

---

[84] COSTA, Fernando José da. ***Locus Delicti* nos crimes informáticos.** 2011. 355 f. Tese (Doutorado em Direito) – Faculdade de Direito da USP, São Paulo, 2011, p. 96/97.
[85] NUCCI, Guilherme de Souza. **Código penal comentado**. 10. ed. rev., atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2010, p. 733.

É explícito a possibilidade de haver crime de furto praticado pela internet, tanto que o Superior Tribunal de Justiça já consolidou seu entendimento nesse sentido.

Para a Corte Superior, a apropriação de valores mediante transferências bancárias fraudulentas com o uso da internet sem a concordância do titular da conta configura furto qualificado pela fraude.

Ressalta-se que a qualificadora da fraude se consuma, nesses casos, com o burlamento dos sistemas de segurança da instituição financeira.

Veja o entendimento da Colenda Corte:

> CONFLITO NEGATIVO DE COMPETÊNCIA. PENAL E PROCESSO PENAL. FRAUDE ELETRÔNICA NA INTERNET. TRANSFERÊNCIA DE NUMERÁRIO DE CONTA DA CAIXA ECONÔMICA FEDERAL. FURTO MEDIANTE FRAUDE QUE NÃO SE CONFUNDE COM ESTELIONATO. CONSUMAÇÃO. SUBTRAÇÃO DO BEM. APLICAÇÃO DO ART. 70 DO CPP. COMPETÊNCIA DA JUSTIÇA FEDERAL PARANAENSE.
> 1. O furto mediante fraude não se confunde com o estelionato. A distinção se faz primordialmente com a análise do elemento comum da fraude que, no furto, é utilizada pelo agente com o fim de burlar a vigilância da vítima que, desatenta, tem seu bem subtraído, sem que se aperceba; no estelionato, a fraude é usada como meio de obter o consentimento da vítima que, iludida, entrega voluntariamente o bem ao agente.
> 2. Hipótese em que o agente se valeu de fraude eletrônica para a retirada de mais de dois mil e quinhentos reais de conta bancária, por meio da "Internet Banking" da Caixa Econômica Federal, o que ocorreu, por certo, sem qualquer tipo de consentimento da vítima, o Banco. A fraude, de fato, foi usada para burlar o sistema de proteção e de vigilância do Banco sobre os valores mantidos sob sua guarda. Configuração do crime de furto qualificado por fraude, e não estelionato.
> 3. O dinheiro, bem de expressão máxima da idéia de valor econômico, hodiernamente, como se sabe, circula em boa parte no chamado "mundo virtual" da informática. Esses valores recebidos e transferidos por meio da manipulação de dados digitais não são tangíveis, mas nem por isso deixaram de ser dinheiro. O bem, ainda que de forma virtual, circula como qualquer outra coisa, com valor econômico evidente. De fato, a informação digital e o bem material correspondente estão intrínseca e inseparavelmente ligados, se confundem. Esses registros contidos em banco de dados não possuem existência autônoma, desvinculada do bem que representam, por isso são passíveis de movimentação, com a troca de titularidade. Assim, em consonância com a melhor doutrina, é possível o crime de furto por meio do sistema informático.
> 4. A consumação do crime de furto ocorre no momento em que o bem é subtraído da vítima, saindo de sua esfera de disponibilidade. No caso em apreço, o desapossamento que gerou o prejuízo, embora tenha se efetivado em sistema digital de dados, ocorreu em conta-corrente da Agência Campo Mourão/PR, que se localiza na cidade de mesmo nome.
> Aplicação do art. 70 do Código de Processo Penal.
> 5. Conflito conhecido para declarar competente o Juízo Federal de Campo Mourão - SJ/PR. (CC 67.343/GO, Rel. Ministra LAURITA VAZ, TERCEIRA SEÇÃO, julgado em 28/03/2007, DJ 11/12/2007, p. 170)

É importante ressaltar que foi muito discutido se a apropriação de bens através da internet é crime de furto mediante fraude ou estelionato, todavia, como se viu, essa conduta não pode representar o delito de estelionato, tendo em vista que nesse caso o consentimento e ilusão da vítima são essenciais, já que a entrega de bens é feita de forma voluntária pela vítima, enquanto o furto por meio da fraude é realizado sem que a vítima tenha conhecimento, principalmente porque os sistemas de defesa dos bancos é que são violados.

Alguns autores, como é o caso de Góis Júnior, entendem que a subtração de softwares não constitui crime de furto, argumentando que a conduta exige a subtração de bem material alheio.[86]

Nesse aspecto já se verifica a ausência de dispositivo legal, pois não há na lei nenhum tipo penal que coíba a respectiva conduta. De fato, a doutrina entende que a "coisa móvel", que faz menção o tipo penal, é "todo e qualquer bem corpóreo suscetível de ser apreendido e transportado de um local para outro"[87].

Ocorre que nenhuma conduta que viole direito alheio pode ficar sem a devida proteção pelo direito penal, cabendo, portanto, ao Poder Legislativo e o Judiciário resolverem essa possível omissão.

3.5.2.2 DO ESTELIONATO

O estelionato é um crime patrimonial cometido através de fraude, ou seja, o sujeito ativo engana a vítima para obter alguma vantagem econômica, tipificado no artigo 171 do Código Penal:

> 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.

Nélson Hungria expôs que:

---

[86] GÓIS JÚNIOR, José Caldas. **O direito na era das redes: a liberdade e o delito no ciberespaço**. Bauru/SP: EDIPRO, 2001, p. 120. *Apud:* COSTA, Fernando José da. ***Locus Delicti* nos crimes informáticos.** 2011. 355 f. Tese (Doutorado em Direito) – Faculdade de Direito da USP, São Paulo, 2011, p. 98.

[87] MASSON, Cleber. **Direito penal esquematizado: parte especial – vol. 2**. 7ª. ed. rev., atual. e ampl. Rio de Janeiro: Forense; São Paulo: MÉTODO, 2015, p. 308/309.

> O estelionato e o crime patrimonial mediante *fraude*: ao invés da *clandestinidade,* da *violência física* ou da *ameaça intimidativa, o* agente emprega o *engano* ou se serve deste para que a vítima, inadvertidamente, se deixe espoliar. E uma forma *evoluída* de captação do alheio. Nos tempos modernos, a fraude constitui o cunho predominante dos crimes contra o patrimônio.[88]

Analisando detidamente o tipo legal, é possível verificar que alguns elementos fundamentais o integram, quais sejam: a) a conduta do agente visa, exclusivamente, obter vantagem ilícita; b) essa vantagem é para si próprio ou terceiro; c) há o induzimento ou manutenção da vítima em erro; d) o sujeito utiliza artifício ardil ou qualquer outro meio de fraude.[89]

A internet e os novos sistemas eletrônicos facilitaram a ação dos estelionatários, que viram inúmeras oportunidades para obterem lucros à custa de outrem, utilizando de artifícios que levam pessoas a erro.

O estelionato no âmbito virtual é praticado por sujeitos que possuem conhecimento técnico em informática e tecnologia, tendo em vista que o *"modus operandi*" é diverso daquele praticado no meio real. Ora, o estelionato virtual ou informático é realizado pela internet, enquanto o real é praticado no mundo físico e pode ser praticado por qualquer pessoa.

Isso não significa que aqueles que não possuam conhecimento técnico não possam praticar estelionato virtual, podem sim, contudo, é pouco provável.

Com efeito, o respectivo delito pode ser praticado através de programas de computador, como é o caso do *"phishing scam"*, utilizado para obter dados pessoais e financeiros das vítimas. Sobre o procedimento, Costa consigna que:

> Visando ainda a obtenção de vantagem patrimonial, através da *internet* surgiu o *phishing sacam;* nele o internauta envia *e-mails* contendo mensagens falsas com o escopo de capturar dados pessoais e financeiros dos destinatários.
> A vítima, no instante em que clica a mensagem fraudulenta, inicia a instalação de um programa malicioso, seguida de uma mensagem de erro. Em seguida são abertas páginas falsas de formulários para a coleta de informações da vítima. No próximo passo, quando o usuário acessar os *sites* bancários, estes serão substituídos para *sites* redirecionados, onde o infrator conhecedor dos dados e senhas pessoais do usuário poderá de qualquer lugar ligado à

---

[88] HUNGRIA, Nélson, FRAGOSO, Heleno Cláudio. **Comentários ao código penal,** v.7, arts. 155 ao 196. 1. ed. Rio de Janeiro: Forense, 1955, p. 159.
[89] GRECO, Rogério. **Curso de direito penal – parte especial, volume III**. 9. ed. Niterói/RJ: Impetus, 2012, p. 237.

> *internet*, acessar sua conta bancária e efetuar operações financeiras como se fosse o usuário. Se, exemplificando, utilizasse um usuário falso ou de outrem ou acessasse a rede através dos denominados sítios de acesso anônimo, as chances de ser identificado seriam mínimas.[90]

A empresa Kaspersky Lab, especializada em antivírus, demonstrou em 2015 que o Brasil libera o "*ranking"* dos usuários que foram atacados pelo *"phishing"*. Segundo a pesquisa 18,28% (dezoito virgula vinte e oito por cento) dos usuários brasileiros já teriam recebido mensagens. Os top cinco são: Brasil (18,28%), Índia (17,73%), China (14,92%), Cazaquistão (11,64%) e Rússia (11,62%).[91]

Há alguns anos criminosos simularam uma citação digital de processo que estaria tramitando no Superior Tribunal de Justiça. O e-mail fingia estar assinado pelo Presidente da Corte e pedia para o usuário seguir um link, que lhes seria disponibilizado mais informações sobre o cancelamento do julgamento e cancelamento do processo.[92]

Por conta disso, o Colendo Tribunal foi obrigado a se manifestar e dizer que o e-mail era falso, tratando de uma pratica criminosa que tinha como objetivo obter dados pessoais dos usuários, conhecido como *"phishing scam"*.

Vê-se, portanto, que "*Cracker"* não medem esforços para obterem vantagens, o que traz preocupação, haja vista a dificuldade que se tem para identificar os sujeitos dessas condutas.

Feita a análise das respectivas condutas criminais, passa-se a análise das principais inovações legislativas, bem como da dificuldade que ainda se tem de repreender os crimes informáticos.

---

[90] COSTA, Fernando José da. ***Locus Delicti* nos crimes informáticos.** 2011. 355 f. Tese (Doutorado em Direito) – Faculdade de Direito da USP, São Paulo, 2011, p. 100.

[91] ROHR, Altieres. **Brasil lidera ranking de usuários atacados por phishing, diz Kaspersky Lab.** Disponível em: http://g1.globo.com/tecnologia/blog/seguranca-digital/post/brasil-lidera-ranking-de-usuarios-atacados-por-phishing-diz-kaspersky-lab.html. Acessado em 20 de set. 2016.

[92] BRASIL, Superior Tribunal de Justiça. **ALERTA: Golpe eletrônico utiliza nome do STJ para roubar dados pessoais**. Disponível em: http://www.stj.jus.br/sites/STJ/default/pt_BR/Comunica%C3%A7%C3%A3o/%C3%9Altimas-not%C3%ADcias/ALERTA:-Golpe-eletr%C3%B4nico-utiliza-nome-do-STJ-para-roubar-dados-pessoais. Acessado em: 20 de set. 2016.

4 INOVAÇÕES LEGISLATIVAS: O ADVENTO DA TUTELA DOS CRIMES INFORMÁTICOS E AS DIFICULDADES NA REPRESSÃO DOS CRIMES

Mesmo não fazendo parte das convenções internacionais que tratam da matéria, como se verá adiante, o Brasil inovou consideravelmente na tutela dos crimes informáticos, embora se tenha muita dificuldade em repreender as condutas, seja pela ausência de lei específica ou pela ineficácia do trabalho desempenhado pelas autoridades competentes, bem como devido a problemas relacionados à competência para julgar o crime.

4.1 CONVENÇÃO DE BUDAPESTE

Inicialmente, é importante ressaltar que há aproximadamente quinze anos muitos países trabalham para coibir os crimes informáticos, tendo em vista o aumento e a dificuldade de repreensão dessas condutas.

A Convenção de Budapeste ou Convenção sobre o Cibercrime foi criada em 2001, no entanto está em vigor desde 2004, sendo signatários mais de vinte países.

Com efeito, o Brasil não integra a respectiva convenção, por isso não usufrui dos benefícios da cooperação internacional.

O teor da Convenção demonstra a necessidade de cooperação entre os Estados (países) no combate à criminalidade informática, haja vista que com a internet não há barreiras territoriais para praticar crimes, conforme demonstrado neste trabalho.

Ocorre que além da cooperação internacional e da indústria privada, a legislação sobre a matéria é de fundamental importância no combate à criminalidade, que deve ser rápida e eficaz, conforme estabelece o preâmbulo da convenção:

> Reconhecendo a importância de intensificar a cooperação com os outros Estados Partes da presente Convenção;
> Convictos da necessidade de prosseguir, com carácter prioritário, uma política criminal comum, com o objectivo de proteger a sociedade contra a criminalidade no ciberespaço, designadamente, através da adopção de legislação adequada e da melhoria da cooperação internacional;
> Conscientes das profundas mudanças provocadas pela digitalização, pela convergência e pela globalização permanente das redes informáticas;
> Preocupados com o risco de que as redes informáticas e a informação electrónica, sejam igualmente utilizadas para cometer infracções criminais e

> de que as provas dessas infracções sejam armazenadas e transmitidas através dessas redes;
> Reconhecendo a necessidade de uma cooperação entre os Estados e a indústria privada no combate à cibercriminalidade, bem como a necessidade de proteger os interesses legítimos ligados ao uso e desenvolvimento das tecnologias da informação;
> Acreditando que uma luta efectiva contra a cibercriminalidade requer uma cooperação internacional em matéria penal acrescida, rápida e eficaz;[93]

A convenção prega ainda a necessidade de respeitar outros acordos internacionais, entre eles, a Convenção para Proteção dos Direitos do Homem e das Liberdades Fundamentais do Conselho da Europa de 1950, o Pacto Internacional sobre os Direitos Civil e Políticos das Nações Unidas de 1966, a Convenção do Conselho da Europa de 1981 (garante a preservação dos dados pessoais), a Convenção das Nações Unidas sobre os Direitos da Criança de 1989, a Convenção da Organização Internacional do Trabalho sobre as Piores Formas do Trabalho Infantil de 1999, e demais convenções que tratam direito penal.

A Convenção sobre o Cibercrime é composta por quatro capítulos: Capítulo I – Terminologia (artigo 1º); Capítulo II – Medidas a tomar a nível nacional (artigos 2º ao 22º); Capítulo III – Cooperação Internacional (artigos 23º ao 35º); e Capítulo IV – Disposições Finais (artigos 36º ao 48º).

Sublinha-se que interessa para este Trabalho os Capítulos II e III, contudo, não será analisado todos os artigos, mas aqueles que se entende como principais.

Por ser uma convenção seu texto expõe o que cada Estado deverá fazer, os artigos 2º a 6º, por exemplo, tratam dos crimes contra à integridade, confidencialidade e disponibilidade dos sistemas e dados informáticos, isto é, a Convenção recomenda que os países signatários tipifiquem no direito interno os atos de acesso ilegítimo intencional, interceptação ilegítima de dados informáticos, interferência em dados, interferência em sistemas e uso abusivo de dispositivos.[94]

Eis o texto da Convenção:

Artigo 2º - Acesso ilegítimo

---

[93] HÚNGRIA. **Convenção sobre o Cibercrime**. Disponível em: http://www.internacional.mpf.mp.br/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf. Acessado em 20 de set. 2016.

[94] MORAIS NETO, Arnaldo Sobrinho de. **Crimes e cooperação penal internacional: um enfoque à luz da convenção de Budapeste.** 2009,. 188 f. Dissertação (Mestrado em Direito) – Universidade Federal da Paraíba - UFPB, João Pessoa/PB, 2009, p. 130.

Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, o acesso intencional e ilegítimo à totalidade ou a parte de um sistema informático. As Partes podem exigir que a infracção seja cometida com a violação de medidas de segurança, com a intenção de obter dados informáticos ou outra intenção ilegítima, ou que seja relacionada com um sistema informático conectado a outro sistema informático.

Artigo 3º - Intercepção ilegítima

Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, a intercepção intencional e ilegítima de dados informáticos, efectuada por meios técnicos, em transmissões não públicas, para, de ou dentro de um sistema informático, incluindo emissões electromagnéticas provenientes de um sistema informático que veicule esses dados. As Partes podem exigir que a infracção seja cometida com dolo ou que seja relacionada com um sistema informático conectado com outro sistema informático.

Artigo 4º - Interferência em dados

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, o acto de intencional e ilegitimamente danificar, apagar, deteriorar, alterar ou eliminar dados informáticos.

2. Uma Parte pode reservar-se o direito de exigir que a conduta descrita no n.º 1 provoque danos graves.

Artigo 5º - Interferência em sistemas

Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, no seu direito interno, a obstrução grave, intencional e ilegítima, ao funcionamento de um sistema informático, através da introdução, transmissão, danificação, eliminação, deterioração, modificação ou supressão de dados informáticos.

Artigo 6º - Uso abusivo de dispositivos

1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracções penais, em conformidade com o seu direito interno, quando cometidas intencional e ilegitimamente:

a) A produção, a venda, a obtenção para utilização, a importação, a distribuição, ou outras formas de disponibilização de:

i. Um dispositivo, incluindo um programa informático, concebido ou adaptado essencialmente para permitir a prática de uma das infracções definidas em conformidade com os artigos 2º a 5º;

ii. Uma palavra-passe, um código de acesso ou dados informáticos semelhantes que permitam aceder a todo, ou a parte de um sistema informático com a intenção de serem utilizados para cometer qualquer uma das infracções definidas nos Artigos 2º a 5º; e

b) A posse de um elemento referido nos alínea *a)*, *i.* ou *ii.*, com a intenção de ser utilizado com o objectivo de cometer qualquer uma das infracções referidas nos artigos 2º a 5º. As Partes podem exigir que no direito interno se reuna um certo número desses elementos para que seja determinada a responsabilidade criminal.

2. O presente artigo não deve ser interpretado como impondo responsabilidade criminal quando a produção, a venda, a aquisição para utilização, a importação, a distribuição, ou outra forma de disponibilização ou posse, mencionadas no n.º1 do presente artigo não tenham por objectivo cometer uma infracção estabelecida em conformidade com os artigos 2º a 5º da presente Convenção, como é o caso de ensaios autorizados ou de protecção de um sistema informático.

3. Cada Parte pode reservar-se o direito de não aplicar o disposto no n.º 1 do presente artigo desde que essa reserva não diga respeito à venda,

> distribuição, ou a qualquer outra forma de disponibilização dos elementos referidos no n.º 1, *a)*, *ii.*[95]

As condutas de acesso ilegítimo, interferência de dados informáticos, interferência em sistemas e uso abusivo de dispositivos não possuem previsão legal no ordenamento jurídico brasileiro, demonstrando, portanto, a carência da legislação brasileiro quanto a criminalização informática.

Outrossim, em relação à administração pública o acesso não autorizado é crime, sendo considerada violação de sigilo funcional. O tipo está descrito no artigo 325, §1º, incisos I e II, do Código Penal, o qual foi inserido pela Lei nº. 9.983/2000:

> **Violação de sigilo funcional**
> Art. 325 - Revelar fato de que tem ciência em razão do cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação:
> Pena - detenção, de seis meses a dois anos, ou multa, se o fato não constitui crime mais grave.
> § 1º Nas mesmas penas deste artigo incorre quem: (Incluído pela Lei nº 9.983, de 2000)
> I – permite ou facilita, mediante atribuição, fornecimento e empréstimo de senha ou qualquer outra forma, o acesso de pessoas não autorizadas a sistemas de informações ou banco de dados da Administração Pública; (Incluído pela Lei nº 9.983, de 2000)
> II – se utiliza, indevidamente, do acesso restrito. (Incluído pela Lei nº 9.983, de 2000)

Observa-se que o respectivo dispositivo legal só dá guarida às violações ocorridas no âmbito da administração público, ou seja, a violação de sigilo profissional só é crime se praticada por funcionário público.

Com efeito, o Poder Legislativo acobertou somente os direitos do Poder Público, deixando à míngua os direitos do particular, que também tem preocupações quando ao acesso não autorizado de dispositivos, ainda que o invasor não obtenha nenhuma informação.

A Lei Carolina Dieckmann (Lei nº. 12.737/2012) tipifica a conduta de invasão de dispositivo informático, contudo, só considera crime se o invasor obter, adulterar ou destruir dados ou informações, cujo análise será realizada no próximo tópico.

---

95 HÚNGRIA. **Convenção sobre o Cibercrime**. Disponível em: http://www.internacional.mpf.mp.br/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs _legislacao/convencao_cibercrime.pdf. Acessado em 20 de set. 2016.

A respeito disso, quer-se dizer o seguinte, embora o invasor não encontre nada útil a seus interesses, as pessoas costumam guardar em seus dispositivos eletrônicos informações, arquivos e até documentos sigilosos, por isso, o simples fato de terceiro não autorizado ter acesso a tais arquivos causa constrangimento e violação à direito, fato que deveria ser considerado crime.

Por outro lado, no tocante à interceptação ilegítima de dados informáticos, a própria Constituição Federal de 1988 preceitua em seu artigo 5º, inciso XII, a inviolabilidade do "(...) sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial (...)", cuja conduta foi tipificada como crime posteriormente pela Lei nº. 9.296/96.[96]

O artigo 10 dessa pela reza que é "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", com pena de reclusão de dois a quatro anos e multa.

Por conseguinte, o artigo 7º da Convenção obriga os Estados a definirem como crime a falsidade informática, isto é, constitui crime o ato de introduzir, alterar, eliminar ou suprimir de forma intencional e ilegítima de dados informáticos, produzindo outros falsos, com o objetivo de que sejam utilizados como se legítimos fossem:

> **Artigo 7º - Falsidade informática**
> Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, a introdução, a alteração, a eliminação ou a supressão intencional e ilegítima de dados informáticos, produzindo dados não autênticos, com a intenção de que estes sejam considerados ou utilizados para fins legais como se fossem autênticos, quer sejam ou não directamente legíveis e inteligíveis. Uma Parte pode exigir no direito interno uma intenção fraudulenta ou uma intenção ilegítima similar para que seja determinada a responsabilidade criminal.[97]

Analisando, mesmo que superficialmente esse tipo penal, é patentemente verificável que na Legislação Brasileira não existe nada parecido, ou seja, não é crime praticar falsidade informática no país.

---

[96] MORAIS NETO, Arnaldo Sobrinho de. **Crimes e cooperação penal internacional: um enfoque à luz da convenção de Budapeste.** 2009,. 188 f. Dissertação (Mestrado em Direito) – Universidade Federal da Paraíba - UFPB, João Pessoa/PB, 2009, p. 131.

[97] HÚNGRIA. **Convenção sobre o Cibercrime**. Disponível em: http://www.internacional.mpf.mp.br/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf. Acessado em 20 de set. 2016.

Tal fato demonstra o quanto a Legislação Brasileiras ainda precisa evoluir, vez que o Direito Internacional já demonstrou preocupação com os crimes informáticos e o país pouco faz para coibi-las, seja pelo momento político e financeiro vivenciado ou pela morosidade dos Poderes Legislativo e Judiciário.

A convenção tutela também os crimes que violam a dignidade sexual das crianças e busca coibir as infrações relacionadas com a pornografia infantil. O artigo 9º estabelece que:

> **Artigo 9º - Infracções relacionadas com pornografia infantil**
> 1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracção penal, em conformidade com o seu direito interno, as seguintes condutas, quando cometidas de forma intencional e ilegítima:
> a) Produzir pornografia infantil com o objectivo da sua difusão através de um sistema informático;
> b) Oferecer ou disponibilizar pornografia infantil através de um sistema informático;
> c) Difundir ou transmitir pornografia infantil através de um sistema informático;
> d) Obter pornografia infantil através de um sistema informático para si próprio ou para terceiros;
> e) Possuir pornografia infantil num sistema informático ou num meio de armazenamento de dados informáticos.
> 2. Para efeitos do n.º 1, a expressão "pornografia infantil" inclui qualquer material pornográfico que represente visualmente:
> a) Um menor envolvido num comportamento sexualmente explícito;
> b) Uma pessoa que aparente ser menor envolvida num comportamento sexualmente explícito;
> c) Imagens realísticas que representem um menor envolvido num comportamento sexualmente explícito;
> 3. Para efeitos do n.º 2, a expressão "menor" inclui qualquer pessoa com idade inferior a 18 anos. Uma Parte, pode, no entanto, exigir um limite de idade inferior, que não será menos que 16 anos.
> 4. Cada Parte pode reservar-se o direito de não aplicar, no todo ou em parte, o disposto nos n.ºs 1, alínea *d)*, e., 2, alíneas *b)* e *c)*.[98]

Nesse aspecto a legislação do país merece elogios, visto que o combate à pornografia infantil é protegida pelo ordenamento jurídicos, notadamente pelo Estatuto da Criança e do Adolescente e pelo Código Penal.

Ademais, é importante frisar que para internet não há barreiras geográficas, ou seja, os crimes podem ser praticados de um continente para o outro, não sendo a distância um problema.

---

[98] HÚNGRIA. **Convenção sobre o Cibercrime**. Disponível em: http://www.internacional.mpf.mp.br/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf. Acessado em 20 de set. 2016.

Não obstante, a problemática reside no momento de determinar qual lei será aplicável, ou seja, qual dos países responsabilizará o criminoso.

Os ideais de Cooperação Internacional e Competência se manifestam no artigo 22 da Convenção, que embora não defina as regras, aponta, isto é, direciona os países para “determinarem qual é a jurisdição mais apropriada para o procedimento legal”:

> **Artigo 22º - Competência**
> 1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer a sua competência relativamente a qualquer infracção penal definida em conformidade com os artigos 2º a 11º da presente Convenção, sempre que a infracção seja cometida:
> a) No seu território; ou
> b) A bordo de um navio arvorando o pavilhão dessa Parte;
> c) A bordo de uma aeronave matriculada nessa Parte e segundo as suas Leis; ou
> d) Por um dos seus cidadãos nacionais, se a infracção for punível criminalmente onde foi cometida ou se a infracção não for da competência territorial de nenhum Estado.
> 2. Cada Parte pode reservar-se o direito de não aplicar ou de apenas aplicar em casos ou em condições específicas, as regras de competência definidas no n.º1, alínea *b)* a alínea *d)* do presente artigo ou em qualquer parte dessas alíneas.
> 3. Cada Parte adoptará as medidas que se revelem necessárias para estabelecer a sua competência relativamente a qualquer infracção referida no artigo 24º, n.º1 da presente Convenção, quando o presumível autor da infracção se encontre no seu território e não puder ser extraditado para outra Parte, apenas com base na sua nacionalidade, após um pedido de extradição.
> 4. A presente Convenção não exclui qualquer competência penal exercida por uma Parte em conformidade com o seu direito interno.
> 5. Quando mais que uma Parte reivindique a competência em relação uma presumível infracção prevista na presente Convenção, as Partes em causa, se for oportuno, consultar-se-ão a fim de determinarem qual é a jurisdição mais apropriada para o procedimento penal.[99]

Ressalta-se que a percepção de competência está intimamente ligada a ideia de soberania, que delimita as áreas jurisdicionais do Estado, de modo a fixar em cada foro a competência para apreciar e julgar pleitos, contudo, essa soberania seria mitigada diante da cooperação internacional, em prol de objetivos maiores.[100]

---

[99] HÚNGRIA. **Convenção sobre o Cibercrime**. Disponível em: http://www.internacional.mpf.mp.br/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf. Acessado em 20 de set. 2016.

[100] MORAIS NETO, Arnaldo Sobrinho de. **Crimes e cooperação penal internacional: um enfoque à luz da convenção de Budapeste.** 2009,. 188 f. Dissertação (Mestrado em Direito) – Universidade Federal da Paraíba - UFPB, João Pessoa/PB, 2009, p. 142.

Morais Neto disserta que se o Brasil fosse signatário da Convenção de Budapeste, as previsões contidas no artigo 22 já teriam sido atendidas, pois ao longo do Código Penal e Código de Processo Penal a matéria relacionada à competência está disciplinada.[101] O autor faz uma breve análise dos artigos 5º, 6º e 7º do Código Penal e do artigo 70 do Código de Processo Penal para obter sua conclusão:

> Os artigos 5º, 6º e 7º do Código Penal brasileiro cuidam das regras sobre territorialidade, lugar do crime e extraterritorialidade. A regra geral é a prevista no art. 5º, que trata do princípio da territorialidade (territorialidade temperada ou moderada, uma vez que faz ressalva aos tratados e convenções de qual o país seja signatário), aplicando-se ao crime cometido no Brasil, a lei penal brasileira.
> Quanto ao lugar do crime o Brasil adotou a teoria mista, pura, unitária ou da ubiquidade, conforme dispõe o art. 6º, decorrendo que o *locus commissi delict* "[...] tanto pode ser o da ação como o do resultado, ou ainda o lugar do bem jurídico atingido.
> Assim, as disposições constantes no art. 7º, do Código Penal brasileiro são exceções à regra geral, ou seja, sujeição à lei nacional ainda que o delito seja cometido no estrangeiro.
> Ademais, no âmbito processual penal a competência *ratione loci* é estatuída pelo art 70, do Código de Processo Penal e "[...] 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.[102]

Por fim, como o Brasil não é signatário da Convenção de Budapeste, não goza dos benefícios oriundos da cooperação internacional, e obviamente, paga caro por isso, em que pese tal fato não lhe retire a obrigação de proteger a sociedade contra todas as espécies de crimes.

4.2 LEI CAROLINA DIECKMANN (LEI Nº. 12.737/2012)

No Brasil, as primeiras normas que tratavam sobre a temática informática tinham relação com a forma de execução dos serviços de internet, contudo, no ano de 2012 adveio a Lei nº. 12.737/2012, conhecida como Lei Carolina Dieckmann, cuja matéria regulatória é eminentemente criminal, a qual acrescentou ao código penal os artigos 154-A e 154-B, bem com alterou a redação dos dispositivos 266 e 298, os quais serão devidamente analisados.

---

[101] MORAIS NETO, Arnaldo Sobrinho de. **Crimes e cooperação penal internacional: um enfoque à luz da convenção de Budapeste.** 2009,. 188 f. Dissertação (Mestrado em Direito) – Universidade Federal da Paraíba - UFPB, João Pessoa/PB, 2009, p. 144.
[102] *Ibidem,* p. 143/144.

A Lei foi apelidada como “Lei Carolina Dieckmann” porque no ano de 2012 a atriz global teve fotos íntimas expostas na internet, após a invasão de seu computador.

Tal fato pressionou o Estado a adotar alguma medida para criminalizar esse tipo de conduta e por conta disso, o Deputado Federal Paulo Teixeira (PT-SP) apresentou o projeto de lei, cujo trâmite legal foi acelerado devido a situação vivenciada pela atriz, que inclusive foi chantageada a pagar a quantia de dez mil reais aos criminosos para que suas fotos não fossem divulgadas, todavia, Carolina não cedeu.[103]

Pois bem, importante fazer o estudo do artigo 154-A e 154-B do Código Penal, que dispõem o seguinte:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> 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.
> **Ação penal**
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

---

[103] SILVA, Alessandra Mara de Freitas; SILVA, Cristian Kiefer da. **O problema da tipificação dos crimes informáticos: aspectos controversos a respeito da aplicação do artigo 154-a da lei nº 12.737/2012 “Lei Carolina Dieckmann”.** Disponível em: http://www.publicadireito.com.br/artigos/?cod=2a5b63fbaadcaa8c. Acessado em: 20 de set. 2016.

O tipo apresenta inúmeros elementos, que juntos caracterizam a conduta criminosa, sendo eles: a) o núcleo do tipo é o verbo invadir; b) o dispositivo informático tem que ser de pessoa alheia; c) o dispositivo pode ou não estar conectado à internet; d) a invasão se dar mediante violação dos mecanismos de segurança; e) a finalidade do crime é obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita da vítima; f) ou obter vantagem ilícita mediante a instalação de vulnerabilidades.[104]

Analisando o tipo é possível verificar que seu objeto jurídico é a privacidade individual e/ou profissional, que além de ser tutelada pelo código penal, encontra subsídio na Constituição Federal, no artigo 5º, inciso X.

Dessa forma analisa Rogério Sanches Cunha:

> O objeto jurídico do crime, como se percebe, é privacidade individual e/ou profissional, resguardada (armazenada) em dispositivo informático, desdobramento lógico do direito fundamental assegurado no art. 5°, X, CF/88: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando o direito de indenização pelo dano material ou moral decorrente de sua violação".[105]

A conduta do delinquente é o ato de invadir dispositivo informático alheio, contudo, a mera invasão não caracteriza crime, é necessário que o agente tenha a intensão de “obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita*”*. Portanto, o elemento subjetivo do crime é o dolo, não podendo ser praticado culposamente, bem como o autor da conduta deve ter uma finalidade especial, conforme nos ensina Rogério Greco:

> A conduta do agente, ou seja, o ato de invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante a violação indevida de mecanismos de segurança deve te sido levada a efeito *com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo.*
> Assim, não é a simples invasão, pela invasão, mediante violação indevida de mecanismo de segurança, que importa na prática de infração penal tipificada no *caput* do art. 154-A do diploma repressivo, mas sim aquela que possui um finalidade especial, ou seja, aquilo que denominamos de especial fim de agir,

[104] GRECO, Rogério. **Curso de direito penal – parte especial, volume II: introdução à teoria geral da parte especial: crimes contra a pessoa**. 11 ed. rev. e atual. Rio de Janeiro: Impetus, 2015, p. 604.
[105] CUNHA, Rogério Sanches. **Manual de direito penal – parte especial (arts. 121 ao 361).** 8 ed. rev. ampl. e atual. Salvador/BA: JusPODIVM, 2016, p. 244.

> que consiste na obtenção, adulteração ou destruição de dados ou informações sem a autorização expressa ou tácita do titular do dispositivo. *Obter* tem o significado de adquirir, alcançar o que desejava, conseguir; *adulterar* diz respeito a alterar, estragar, modificar o conteúdo, corromper; *destruir* quer dizer aniquilar, fazer desaparecer, arruinar.[106]

Ademais, trata-se de crime comum, portanto, pode ser praticado por qualquer pessoa, em que pese o conhecimento técnico em informática seja fundamental, já que os principais autores do delito são os *crackers.* Igualmente, o sujeito passivo também pode ser qualquer pessoa, física ou jurídica.[107]

O termo vulnerabilidade indica a instalação de falhas no *software* ou no sistema operacional do dispositivo eletrônico, sendo, portanto, uma ameaça para o dispositivo e para o titular. Isso pode ocorrer com a colocação de um vírus que contribuía com a invasão do sistema para obtenção de informações particulares e confidenciais da vítima.

Dessa maneira, é o que expõe o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil:

> Uma vulnerabilidade é definida como uma condição que, quando explorada por um atacante, pode resultar em uma violação de segurança. Exemplos de vulnerabilidades são falhas no projeto, na implementação ou na configuração de programas, serviços ou equipamentos de rede.
> Um ataque de exploração de vulnerabilidades ocorre quando um atacante, utilizando-se de uma vulnerabilidade, tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais, disparar ataques contra outros computadores ou tornar um serviço inacessível.[108]

Ademais, conforme se observa analisando o tipo, dependendo da conduta praticada pelo agente, o crime poder ter sua pena majorada. O §3º do mencionado artigo prevê a modalidade qualificada da conduta, caso a invasão resulta na obtenção de conteúdo de comunicação telefônica privada, segredos, informações sigilosas ou controle remoto do dispositivo invadido.

De se ressaltar que ainda assim o crime será processado na forma da Lei nº. 9.099/95, por se tratar de infração penal de menor potencial ofensivo, devendo a ação

---

[106] GRECO, Rogério. **Curso de direito penal – parte especial, volume II: introdução à teoria geral da parte especial: crimes contra a pessoa**. 11 ed. rev. e atual. Rio de Janeiro: Impetus, 2015, p. 606.
[107] MASSON, Cleber. **Direito penal esquematizado: parte especial – vol. 2**. 7ª. ed. rev., atual. e ampl. Rio de Janeiro: Forense; São Paulo: MÉTODO, 2015, p. 278.
[108] Cento de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Cartilha de segurança para internet.** Disponível em: http://cartilha.cert.br/ataques/. Acessado em 20 de set. 2016.

penal ser processada mediante representação do ofendido ou do representante legal, salvo se o delito for praticado contra a Administração Pública direta ou indireta, bem como contra as concessionárias de serviço público, nos termo do artigo 154-B do Código Penal citado acima.

Muitos estudiosos criticam o dispositivo legal, aduzindo que o legislador deixou inúmeras “brechas”, seja pela pressa na promulgação da lei devido a forte pressão da mídia, ou mesmo pela inexperiência quanto à matéria.

Renato Opice Blum, por exemplo, critica a utilização do verbo invadir - núcleo do tipo -, destacando que a violação a sistema informático deveria ser violenta, à força, isto é, deveria haver, necessariamente, a violação de determinada barreira para a consumação da conduta, o que não acontece em todos os casos, tendo em vista que nem todos os usuários possuem antivírus poderosos que viabilizem uma real proteção do dispositivo.

Eis o que expõe o nobre advogado:

> Importa analisar, também, os pressupostos da conduta "*invadir"*. Este verbo conceitualmente traz a ideia de *entrada à força*, *ingresso hostil*, *violação de barreira*. Portanto, casos de obtenção indevida de dados através de técnicas de engenharia social e outros meios (divulgação de senha pelo próprio titular do bem a terceiros, por exemplo) em tese não estariam enquadrados na tipificação recém-nascida. Isto porque não haveria qualquer violação, mas apenas o acesso não autorizado.
> Infere-se, deste modo, que todas as hipóteses de aumento de pena relacionadas à prática*invadir*, previstas nos parágrafos do artigo 154-A (*obtenção de comunicações privadas, divulgação dos dados...*) devem ser precedidas pela *violação do mecanismo de segurança*. Não haverá crime, deste modo, nos casos de obtenção e divulgação indevida de dados, quando o agente tem livre acesso ao dispositivo eletrônico da vítima (técnico de TI da empresa, companheiro, colega de trabalho...).[109]

Ainda nesse sentido, o advogado Luiz Augusto Sartori de Castro preceitua que:

> (...) O que colocamos em xeque é a produção de lei motivada pela casuística — aqui, o caso da atriz Carolina Dieckmann — e que, por assim ser, peca e muito na qualidade técnica de sua redação.
> Como exemplo, vale mencionar o verbo nuclear da proposta ao artigo 154-A, qual seja: “invadir*”*. Segundo o dicionário Aurélio, o verbo “invadir” significa “entrar à força, apoderar-se violentamente”. Assim, a subsistir a redação do novel artigo 154-A, somente se poderia cogitar da ocorrência de crime se, e somente se, o agente acessasse o dispositivo de informática

[109] BLUM, Renato Opice. **Crimes eletrônicos – a nova lei é suficiente?** Disposível em: http://www.migalhas.com.br/dePeso/16,MI172711,101048-Crimes+eletronicos+a+nova+lei+e+suficiente. Acessado em: 20 de set. 2016.

> à força, violentamente, em especial porque, em matéria de Direito Penal, a interpretação deve sempre ser restritiva.
> Ocorre que a prática desses atos atentatórios que o artigo 154-A visa a coibir, por excelência, nunca — ou quase nunca — ocorre unilateralmente, isto é, com o agente mal-intencionado tendo agido sozinho para acessar o sistema operacional. É que existem somente dois meios de acessar o banco de dados de um computador de modo indevido: 1) acessando fisicamente o próprio computador — o que é óbvio não se enquadra do tipo penal sob exame; ou 2) quando o usuário permite inadvertidamente que sejam instalados em seu computador os chamados *malwares*, que estão sorrateiramente ocultos em arquivos enviados por e-mails, em determinados links de internet ou em dispositivos móveis como pendrives.[110]

Ao que parece, seria melhor se o termo utilizado pelo tipo fosse substituído por "ter acesso" ou "acessar", já que nem sempre o acesso ao dispositivo alheio é feito com violência, conforme ressaltam Alessandra Mara de Freitas e Cristian Kiefer da Silva:

> Vale ressaltar que devemos ter a ciência de que "*invadir*" e "*ter acesso*", são situações distintas, uma vez que se pode ter acesso a determinados sistemas informáticos sem, necessariamente, invadi-los, como por exemplo, quando clicamos sobre um nome qualquer na lista de usuários do wi-fi, estamos entrando em contato com o roteador (sistema informático) alheio, sem com isso, estarmos invadindo.[111]

Outra crítica, já feita anteriormente, está no fato da necessidade de haver a obtenção, adulteração ou destruição de dados ou informações, isto é, o mero ato de invadir não é crime, o que é um absurdo.

Com efeito, isso é fruto da pressa do Legislador em atender as necessidades de uma pessoa, nesse caso, uma atriz com visibilidade nacional, já que trabalha na maior emissora de televisão do país (Globo). Do modo que está, a lei é lacunosa e deixa de punir inúmeros criminosos, cuja necessidade é premente.

Além disso, os juristas criticam a cominação das penas, que são ínfimas:

> (...) Além das imperfeições na redação dos tipos, as penas cominadas na nova lei são ínfimas se considerada a potencial gravidade das condutas

---

[110] CASTRO, Luiz Augusto Sartori de. **"Lei Carolina Dieckmann" seria a salvação da internet?**. Disponível em: http://www.migalhas.com.br/dePeso/16,MI167980,81042-Lei+Carolina+Dieckmann+seria+a+salvacao+da+internet. Acessado em: 21 de set. 2016.

[111] SILVA, Alessandra Mara de Freitas; SILVA, Cristian Kiefer da. **O problema da tipificação dos crimes informáticos: aspectos controversos a respeito da aplicação do artigo 154-a da lei nº 12.737/2012 "Lei Carolina Dieckmann".** Disponível em: http://www.publicadireito.com.br/artigos/?cod=2a5b63fbaadcaa8c. Acessado em: 20 de set. 2016.

> incriminadas, bastando dizer que um ataque de denegação de serviço pode colocar em risco vidas de uma população inteira.[112]

De fato a pena está muito aquém da realidade. Ora, o crime detém um potencial ofensivo absurdo e pode causar danos irreversíveis à vítima, um exemplo disso é que até hoje, cinco anos depois, fotos da atriz Carolina Dieckmann nua circulam pela internet e provavelmente permaneceram no mundo virtual “eternamente”.

Blum identifica que a falta de definição legal prejudica a repressão do crime. Segundo ele, a lei se limitou em criminalizar a violação indevida de dispositivos de segurança, e, portanto, a violação de sistemas que não possuam segurança não pode ser penalizada. Assim, versa:

> (...) a lei restringiu a tipicidade da conduta aos casos em que há a *violação indevida de mecanismos de segurança*. Assim, podemos entender que todos os dispositivos informáticos não dotados de ferramenta de proteção estariam excluídos do âmbito desta aplicação legal. Além disso, vale pontuar que, como as expressões "*mecanismo de segurança"* e "*dispositivo informático"* (só hardwares? E os softwares?) não foram definidas na lei, pode restar dúvidas sobre o completo enquadramento penal de certos casos.

Diante disso, percebe-se que embora a legislação esteja avançando a seu tempo, a necessidade de aperfeiçoamento é fundamental para que a norma seja eficaz e, de fato, puna quem mereça. A pena aplicada a estes crimes merecem revisão.

4.3 MARCO CIVIL DA INTERNET (LEI Nº. 12.965/2014)

Marco Civil da Internet têm como corpo-diretriz a atribuição de um organismo normativo que institua princípios norteadores para a manutenção dos direitos, deveres e garantias promulgados no texto lei, que apresenta logo em seu artigo 3º, os princípios correlatos a este regulamento.

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;

---

[112] SILVA, Alessandra Mara de Freitas; SILVA, Cristian Kiefer da. **O problema da tipificação dos crimes informáticos: aspectos controversos a respeito da aplicação do artigo 154-a da lei nº 12.737/2012 “Lei Carolina Dieckmann”.** Disponível em: http://www.publicadireito.com.br/artigos/?cod=2a5b63fbaadcaa8c. Acessado em: 20 de set. 2016.

> II - proteção da privacidade;
> III - proteção dos dados pessoais, na forma da lei;
> IV - preservação e garantia da neutralidade de rede;
> V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
> VII - preservação da natureza participativa da rede;
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.

O dispositivo legal deixa claro o contexto altamente constitucionalizado da norma, que não busca individualizar suas atribuições unicamente em seu texto normativo, de modo que outros diplomas legais serão considerados no momento de fazer a interpretação da lei, conforme se extrai da análise do parágrafo único do artigo 3º e artigo 6º da Lei nº. 12.965/2014:

> Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.
> (...)
> Art. 6º Na interpretação desta Lei serão levados em conta, além dos fundamentos, princípios e objetivos previstos, a natureza da internet, seus usos e costumes particulares e sua importância para a promoção do desenvolvimento humano, econômico, social e cultural.

O professor Carlos Eduardo Elias de Oliveira preleciona que o Marco Civil é um dos pontos normativos que regulam o comportamento do indivíduo no mundo virtual, justamente por isso não pode ser analisado isoladamente pelo fato de se tratar de norma específica. Entende ainda, que eventuais conflitos entre o Marco Civil e outras leis devem ser resolvidos com vistas à moderna teoria do Diálogo das Fontes:

> O Marco Civil não é (e nem quis ser) uma ilha normativa deserta, isolada das demais fontes jurídicas. Ele é um dos vários pontos de irradiação normativa que disciplina o comportamento dos indivíduos no mundo virtual.
> A Constituição Federal, como lei fundamental do nosso País, dá as coordenadas principiológicas incontestes do ordenamento jurídico, ao fluxo da qual tramitarão as interpretações que transbordarão do Marco Civil da Internet. Trata-se de uma consequência do que se convencionou batizar de constitucionalização do diversos ramos do Direito.
> (...)
> A resposta a eventuais conflitos entre o Marco Civil da Internet e outros diplomas legais não deverão ser buscados apenas nos critérios tradicionais de solução de antinomias (como o da especialidade e o cronológico), mas

> também na moderna teoria do *Diálogo das Fontes*, fartamente acatada pela doutrina e pela jurisprudência do STJ. [113]

A teoria do Diálogo das Fontes impulsiona a noção de que o Direito deve ser interpretado como um todo, isto é, a norma jurídica não pode ser interpretada de maneira que exclua a aplicação de outra. Noutro giro, o ordenamento jurídico deve ser analisado sistematicamente e de maneira coordenada, a fim de evitar que normas não sejam aplicadas simplesmente pelos critérios de hierarquia, especialidade e cronologia (teoria clássica).

Ocorre que o ponto de maior controvérsia contido na Lei do Marco Civil da Internet está na possível "soberania" da liberdade de expressão, que retira a responsabilização da propagação de conteúdos impróprios (ilícitos) dos provedores.

Com efeito, essa conclusão pode ser facilmente extraída a partir da análise do artigo 19 da respectiva lei:

> Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.
> § 1º A ordem judicial de que trata o **caput** deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material.
> § 2º A aplicação do disposto neste artigo para infrações a direitos de autor ou a direitos conexos depende de previsão legal específica, que deverá respeitar a liberdade de expressão e demais garantias previstas no art. 5º da Constituição Federal.
> § 3º As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de internet, poderão ser apresentadas perante os juizados especiais.
> § 4º O juiz, inclusive no procedimento previsto no § 3º, poderá antecipar, total ou parcialmente, os efeitos da tutela pretendida no pedido inicial, existindo prova inequívoca do fato e considerado o interesse da coletividade na disponibilização do conteúdo na internet, desde que presentes os requisitos de verossimilhança da alegação do autor e de fundado receio de dano irreparável ou de difícil reparação.

---

[113] OLIVEIRA, Carlos Eduardo Elias de. **Aspectos Principais da Lei nº 12.965, de 2014, o Marco Civil da Internet: subsídios à comunidade jurídica**. Brasília: Núcleo de Estudos e Pesquisas/CONLEG/ Senado, abr./2014, p. 05/06.

Além da visível violação de direito sob o primado da liberdade de expressão, a lei está em dissonância com o entendimento jurisprudencial.

De se destacar que, segundo consta na lei, o provedor só será responsabilizado se, após ordem judicial específica, não tomar providências para eliminar o conteúdo ilícito, ou seja, o prejudicado deverá pleitear judicialmente a indisponibilidade do conteúdo. Esse conteúdo pode ser fotos, comentários ofensivos ou falsos, documentos, incitações criminosas, etc.

Antes da vigência da Lei do Marco Civil da Internet, o Superior Tribunal de Justiça havia pacificado o entendimento de que o simples pedido de indisponibilidade do conteúdo feito ofendido, no âmbito administrativo, seria suficiente para obrigar o provedor de aplicações a retirá-los do mundo virtual, ou seja, a proscrição do material ofensivo deveria ser realizada independentemente de decisão judicial. Eis o teor da decisão proferida:

> RESPONSABILIDADE CIVIL. INTERNET. REDES SOCIAIS. MENSAGEM OFENSIVA. CIÊNCIA PELO PROVEDOR. REMOÇÃO. PRAZO.
> 1. A velocidade com que as informações circulam no meio virtual torna indispensável que medidas tendentes a coibir a divulgação de conteúdos depreciativos e aviltantes sejam adotadas célere e enfaticamente, de sorte a potencialmente reduzir a disseminação do insulto, minimizando os nefastos efeitos inerentes a dados dessa natureza.
> 2. Uma vez notificado de que determinado texto ou imagem possui conteúdo ilícito, o provedor deve retirar o material do ar no prazo de 24 (vinte e quatro) horas, sob pena de responder solidariamente com o autor direto do dano, em virtude da omissão praticada.
> 3. Nesse prazo de 24 horas, não está o provedor obrigado a analisar o teor da denúncia recebida, devendo apenas promover a suspensão preventiva das respectivas páginas, até que tenha tempo hábil para apreciar a veracidade das alegações, de modo a que, confirmando-as, exclua definitivamente o perfil ou, tendo-as por infundadas, restabeleça o seu livre acesso.
> 4. O diferimento da análise do teor das denúncias não significa que o provedor poderá postergá-la por tempo indeterminado, deixando sem satisfação o usuário cujo perfil venha a ser provisoriamente suspenso. Cabe ao provedor, o mais breve possível, dar uma solução final para o caso, confirmando a remoção definitiva da página de conteúdo ofensivo ou, ausente indício de ilegalidade, recolocando-a no ar, adotando, nessa última hipótese, as providências legais cabíveis contra os que abusarem da prerrogativa de denunciar.
> 5. Recurso especial a que se nega provimento. (EDcl no REsp Nº 1.323.754-RJ (2012/0005748-4), Rel. Ministra NANCY ANDRIGHI, TERCEIRA TURMA, julgado em 17/10/2013)

Com efeito, é público e notório que processos judiciais são morosos e o tempo pode causar problemas irreversíveis ao prejudicado, que anseia e necessita da tutela jurisdicional. Assim, a obrigatoriedade de tutelar judicialmente a retirada de material

inapropriado pode tornar ineficiente a própria decisão, como também inatingível o objetivo do pleiteante.

Na prática, o Marco Civil "promove a conduta irrazoável e irresponsável de provedores de serviços na internet"[114], tendo em vista que mesmo sendo negligentes, só serão responsabilizados se descumprirem ordem judicial.

Ressalta-se que a única exceção à regra contida no artigo 19 está no dispõe o artigo 21, que se refere à divulgação de vídeos, imagens ou outros materiais que possuam conotação sexual. Nesses casos, não é exigido do ofendido a propositura de ação judicial, sendo suficiente a notificação do provedor:

> Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.

Não obstante, a velocidade com que as informações se propagam na rede clama por medidas rápidas e eficazes para coibir a divulgações de conteúdos ofensivos. A necessidade de pedido judicial com certeza não é uma dessas medias, assim como o fundamentado na liberdade de expressão não é suficiente para essa exigência.

Consigna-se que a liberdade de expressão não é soberana frente a violações de outros direitos, principalmente tidos como fundamentais, como é o caso da inviolabilidade da hora.

Não obstante, tratar da responsabilização desta forma é perdurar a insensibilidade dos corpos normativos, tornando a resolução factual dos problemas gerados por conteúdos puramente indecorosos impossíveis, conservando os prejuízos gerados, neste sentido Marcelo Thompson versa:

> Mas por que dizer que o Marco Civil prioriza a liberdade de expressão sobre outros direitos? Porque, para promovê-la, o Marco Civil busca neutralizar qualquer papel que os intermediários, os guardiões dos portais por onde o

[114] THOMPSON, Marcelo, **Marco civil ou demarcação de direitos? Democracia, razoabilidade e as fendas na internet do Brasil,** rda – revista de Direito Administrativo, Rio de Janeiro, v. 261, p. 203-251, set./dez. 2012, p. 214.

> conhecimento — mas também ignorâncias e mazelas de toda sorte — circulam na internet, possam desempenhar na preservação de direitos. A premissa fundamental é a de que os intermediários — como o Youtube e o Facebook — não devem ter qualquer dever de guardar a razoabilidade e a responsabilidade jurídicas de seus próprios usuários, pois isso violaria a liberdade de expressão. Em outras palavras, mesmo quando o Youtube e o Facebook saibam que hospedam conteúdo que viola a vida privada e a reputação das pessoas — isto é, mesmo quando alguém tanto já lhes tenha dito expressamente e demonstrado de maneira robusta —, eles não têm qualquer responsabilidade de examinar a natureza do conteúdo e lhe dar atenção compatível com a seriedade dos direitos cuja proteção se busca.[115]

Todavia, o contexto geral desta lei é benéfico, pois dispõe de deveres e direitos, apesar de já existentes em termos jurisprudências, agora, firmados por norma promulgada, contudo para a real eficácia da aplicação deste dispositivo, somente a norma posta não será o suficiente, a criação de mecanismos e institutos para a manutenção do ordenado se faz necessário, o aparelhamento estatal é imprescindível, assim como afirmam Arthur Bezerra e Igor Waltz:

> Por delimitar direitos e responsabilidades de usuários, a partir das demandas da sociedade enviadas por meio de consultas públicas, o Marco Civil da Internet representa um importante avanço na governança da rede no país. Todavia, exatamente por conta do caráter global da rede, medidas legais de segurança perdem efetividade se não forem acompanhadas de devidos avanços de infraestrutura. O Marco Civil constitui talvez uma das pedras fundamentais para a promoção da liberdade de expressão, combate à censura e promoção de direitos constitucionais da internet, mas não encerra o debate, uma vez que é preciso avançar em termos técnicos, políticos, legais e sociais. A efetividade de uma legislação para a rede depende que o governo produza, em curto prazo, uma série de regulamentações que instituirão os detalhes de como serão tratados temas centrais do novo arcabouço jurídico, como liberdade de expressão, segurança de dados e, especialmente, direitos de autor e copyright, que dependerão de leis ainda a serem criadas. Somente dessa forma será possível caminhar para que os avanços propostos pelo marco se tornem efetivos e as suas deficiências sejam superadas.[116]

Por fim, cabe expor que outros aspectos do Marco Civil da Internet merecem atenção da jurisprudência e da doutrina, em detrimento das dissonâncias existentes na Lei, principalmente no que diz respeito a responsabilidade civil, contudo, o objeto desse trabalho trata especificamente dos aspectos e dificuldade de repressão dos crimes informáticos.

---

[115] THOMPSON, Marcelo, **Marco civil ou demarcação de direitos? Democracia, razoabilidade e as fendas na internet do Brasil,** rda – revista de Direito Administrativo, Rio de Janeiro, v. 261, p. 203-251, set./dez. 2012, p. 212/213.

[116] BEZERRA , Arthur C.; WALTZ, Igor. **Privacidade, neutralidade e inimputabilidade da internet no Brasil,** Revista Eptic Online Vol.16 n.2 p.161-175.

4.4 A INCAPACIDADE PROFISSIONAL E TÉCNICA DOS ÓRGÃOS DE INVESTIGAÇÃO

Os delitos informáticos demandam uma capacidade profissional avançada para seu combate, identificação e repressão do crime, contudo, o país ainda precisa evoluir muito para que isso ocorra efetivamente.

Identificar o sujeito ativo do crime ainda é a maior dificuldade, por isso os peritos criminais precisam estar bem capacitados, tendo em vista que a prova pericial é fundamental para determinar a materialidade do crime e sua autoria.

Emerson Wendt, Delegado de polícia, expõe numa entrevista feita ao G1, que os papéis da polícia no combate aos crimes informáticos se manifestam na repressão e prevenção, contudo, a polícia precisa de mais treinamento, equipamentos e ferramentas para cumprir seus objetivos. Ressalta ainda, a necessidade da criação de mais delegacias especializadas, com profissionais altamente preparados para lidar com os crimes.

Faz-se necessário transcrever trechos da entrevista mencionada:

> Acredito que são dois os papeis da Polícia no mundo virtual: agir de modo a reprimir os delitos, investigando-os, e, também atuar constantemente no aspecto preventivo, orientando os usuários quanto ao melhor uso na internet, evitando que sejam vítimas de algum crime virtual.
> (...)
> Acho que a Polícia precisa de mais treinamento e agentes policiais em investigação, além de equipamentos e ferramentas adequadas. Sentimos, também, falta de mais peritos formados na área, justamente para que possam comparecer e realizar o que chamamos de perícia online.
> (...)
> Acho que a Polícia precisa de mais treinamento e agentes policiais em investigação, além de equipamentos e ferramentas adequadas. Sentimos, também, falta de mais peritos formados na área, justamente para que possam comparecer e realizar o que chamamos de perícia online. Acredito que para 2011 - se o planejamento dependesse só de mim - o ideal seria termos ao menos uma Delegacia de Polícia em cada Estado, interagindo e trabalhando em conjunto no combate aos crimes praticados no ambiente virtual.[117]

Como visto, a criminalidade informática aumenta e se especializa a cada dia, o que não acontece com a legislação brasileira, que é lacunosa e insuficiente, isto é, o

[117] ROHR, Altieres. **Trabalho Contra Crimes Virtuais Ainda Está Longe do Ideal, Diz Delegado**. G1-Tecnologia, 06 jan. 2011. Disponível em: http://g1.globo.com/tecnologia/noticia/2011/01/trabalho-contra-crimes-virtuais-ainda-esta-longe-do-ideal-diz-delegado.html. Acessado em 21 de set. 2016.

ordenamento jurídico brasileiro não está preparado para combater todos os crimes praticados no âmbito informático.

Nada obstante, o mesmo ocorre no âmbito investigativo, cuja ausência de especialização está contribuindo para a prática dos crimes, por conta disso, melhorar substancialmente os meios investigativos e repressivos é medida necessária e urgente, como roga Adalton de Almeida Martins:

> O chefe dessa divisão da PF, delegado Adalton de Almeida Martins, admite que o Brasil está atrasado no combate aos crimes praticados na rede mundial de computadores. "Ou a gente se especializa nisso, nas unidades Policiais, na Polícia Federal e nas Polícias Civis que já estão trabalhando nesses crimes em alguns Estados, ou vamos perder a guerra".[118]

Ademais, é inegável a preocupação dos Poderes Públicos, conduto, a criação de delegacias especializadas, conforme prevê a Lei Azeredo (Lei nº. 12.735/2012)[119] não resolverá o problema. É imprescindível a realização de capacitações contínuas, por profissionais especializados, fazendo com que os órgãos persecutórios reprimam e acompanhem a evolução dos crimes.[120]

Outrossim, políticas públicas nacionais que incentivem e contribuam para a qualificação dos profissionais também precisam ser implementadas pelo país.

Com efeito, a coleta inadequada de provas, pode provocar sua invalidade devido sua fragilidade, bem como pode chegar a lugar nenhum, ou seja, provas frágeis contribuem com a impunidade do criminoso.

Santos e Fraga ensinam o seguinte:

> Vale ressaltar que quase todo crime cometido, no qual há um computador relacionado, se as provas digitais não forem coletadas adequadamente, sem as ferramentas técnicas apropriadas, podem ser invalidadas em possível litígio judicial. As a prova digital é extremamente frágil, de forma que, se não

---

[118] SANTOS, Coriolano Aurélio de Almeida Camargo; FRAGA, Ewelyn Schots. **As Múltiplas Faces dos Crimes Eletrônicos e dos Fenômenos Tecnológicos e Seus Reflexos no Universo Jurídico.** São Paulo: OAB SP, 2010, p. 48.

[119] O artigo 4º da Lei expõe que: “Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado. ”

[120] WENDT, Emerson, JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos: ameaças e procedimentos de investigação.** 2. ed. Rio de Janeiro: Brasport, 2013, p. 237.

> tratada dentro de padrões técnicos específica que não deixe rastros para dúvidas, ela pode perfeitamente ser contestada pelo acusado e anulada.[121]

Por fim, é possível observar diariamente que os criminosos mantêm uma relação organizacional, isto é, embora espalhados em diversas localidades, as ações criminosas são realizadas em parceria, o que dificulta a investigação, bem como a identificação dos sujeitos.

No entanto, o mesmo não ocorre entre os órgãos responsáveis pela repressão dos crimes, pois "não existe uma atuação integrada entre os responsáveis pela persecução penal, mesmo aqueles pertencentes ao mesmo setor."[122]

Disserta-se que não há justificativa para essa prática, considerando que todos os órgãos visam o mesmo objetivo, qual seja, reprimir e prevenir condutas delituosas.

Os país precisa evoluir para poder reprimir com veemência os crimes informáticos; cursos, especializações, políticas públicas de incentivo e acordos internacionais precisam ser incorporados, pois a sociedade carece da tutela do Estado, que deve ser qualificada a fim de conceder ao povo a paz social esperada.

4.5 O PROBLEMA DA COMPETÊNCIA

Além da ausência de legislação específica para inúmeras condutas, bem como a falta de preparo das policias investigativas, a delimitação de competência para análise dos crimes informáticos é um dos principais problemas enfrentados pelo direito internacional, cuja solução não está próxima.

Celso Valin, citado por Marina Giantomassi Della Torre expõe e questiona que:

> (...) o grande problema ao se trabalhar com o conceito de jurisdição e territorialidade na Internet, reside no caráter internacional da rede. Na Internet não existem fronteiras e, portanto, algo que nelas esteja publicado estará em todo o mundo. Como, então, determinar o juízo competente para analisar um caso referente a um crime ocorrido na rede?[123]

---

[121] SANTOS, Coriolano Aurélio de Almeida Camargo; FRAGA, Ewelyn Schots. **As Múltiplas Faces dos Crimes Eletrônicos e dos Fenômenos Tecnológicos e Seus Reflexos no Universo Jurídico.** São Paulo: OAB SP, 2010, p. 78.

[122] WENDT, Emerson, JORGE, Higor Vinicius Nogiueira. **Crimes cibernéticos: ameaças e procedimentos de investigação.** 2. ed. Rio de Janeiro: Brasport, 2013, p. 238.

[123] VALIN, Celso. **A questão da jurisdição e da territorialidade nos crimes praticados pela internet.** *In:* ROVER, Aires José (organizador). **Direito, sociedade e informática: limites e perspectivas da vida digital.** Florianópolis: Fundação Boiteux, 2000, p. 115. *Apud:* TORRE, Marina Giantomassi Della.

Como se sabe, os crimes praticados por meio da internet podem atingir inúmeras pessoas, em várias localidades, além de poder incidir sobre várias legislações, o que obsta o processamento e condenação do criminoso, ante a dificuldade de indicar o juízo competente, haja vista que todos os prejudicados (Estados) possuem interesse em responsabilizar o criminoso.

Para demonstrar a dificuldade que se tem para estabelecer uma jurisdição dos crimes informáticos, Christiante Pegorari Conte traz à baila o caso *Yahoo* França. Trata-se de um site no qual uma pessoa vendia produtos nazistas pelo mundo, estando hospedado nos Estados Unidos da América. A jurisdição francesa chamou para si a responsabilidade sob o argumento de que os efeitos repercutiram diretamente no país, contudo, isso não resolve o problema, já que inúmeros países foram atingidos pela conduta ilícita.[124]

Com efeito, pode-se verificar o quão intrincado está o problema da delimitação de jurisdição e competência nos delitos informáticos. A maioria dos ordenamentos jurídicos do mundo, inclusive o brasileiro, adotaram, no que se refere ao lugar do crime, a teoria da ubiquidade para definir a jurisdição competente. De acordo com essa teoria, prevista no artigo 6º do Código Penal: "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. "

Assim, lugar do delito é tanto aquele em que a ação foi realizada, no todo ou em parte, como aquele cujo resultado foi ou deveria ter sido produzido. A aplicação dessa teoria justifica-se no fato de que antes da internet a conduta e o resultado eram produzidos dentro do mesmo território, todavia, com o advento da rede mundial de computadores e a criminalidade informática transnacional, a teoria causa conflitos entre os Estados e nada resolve.[125]

Aspectos processuais e penais dos crimes de computador. 2009. 183 f. Dissertação (Mestrado em Direito Processual Penal), São Paulo, 2009, p. 102.

[124] CONTE, Christiany Pegorari. **Jurisdição e competência nos crimes informáticos.** Revista Brasileira de Meio Ambiente Digital e Sociedade da Informação. V. 01, nº. 01, p. 49-208, 2014, p. 152/153.

[125] COSTA, Fernando José da. ***Locus Delicti* nos crimes informáticos.** 2011. 355 f. Tese (Doutorado em Direito) – Faculdade de Direito da USP, São Paulo, 2011, p. 150.

À vista disso, é patente a necessidade de adoção de documentos internacionais sobre o assunto, aptos para solucionar a questão da competência.

Henry Perrit defende a criação de Cortes Criminais Internacionais, as quais, segundo ele, poderiam solucionar o problema dos conflitos de competência, contudo, para isso seria fundamental que os crimes reprimidos fossem amplamente debatidos por todos os países.[126]

Ademais, a dificuldade na fixação da competência somada a diversidade de legislações por beneficiar o criminoso e lavá-lo à impunidade, dificultando o combate à criminalidade. A respectiva impunidade pode ser reflexo da ausência de criminalização de determinada conduta em outro país ou pelo fato da pena ser menos grave.

Não obstante, cabe ressaltar que o problema da competência reside no âmbito da criminalidade informática transnacional, pois no âmbito interno as normas que tratam da questão são suficientes para fixação do juízo competente, devendo o interprete analisar os crimes informáticos da mesma maneira que faz com relação aos demais delitos, consoante os ensinamentos de Rossini:

> Para fixar a competência de uma infração penal telemática, o operador deverá formular raciocínio idêntico ao que faz com relação aos crimes ditos tradicionais: se material, formal, de mera conduta; se tentado, consumado etc. (...) as normas de fixação de competência existentes não necessitam de qualquer alteração para tratar das infrações penais telemáticas. Basta boa vontade do operador que, repita-se, deve conhecer direito material para classificar exatamente o delito que a ele se apresenta.[127]

Insta destacar que são muitas as ideias para solucionar esse problema, contudo, até agora nada de concreto foi realizado. Os crimes informáticos violam inúmeros bens jurídicos, como a vida, privacidade, segurança de sistemas financeiros, etc., por isso alguma medida urgente precisa ser tomada, pois a ausência de reprimenda penal, devido a impossibilidade de atribuir a competência, provoca a impunidade do sujeito.

---

[126] PERRIT JR, Henry H. **Jurisdiction in Cyberspace**. Pensilvania: Villanova University School of law, 1995, *apud,* GOUVÊA, Sandra. **O direito na era digital: crimes praticados por meio da informática.** Rio de Janeiro: Mauad, 1997, p. 103. *Apud:* TORRE, Marina Giantomassi Della. **Aspectos processuais e penais dos crimes de computador.** 2009. 183 f. Dissertação (Mestrado em Direito Processual Penal), São Paulo, 2009, p. 109.

[127] ROSSINI, Augusto Eduardo de Souza. **Informática, Telemática e Direito Penal.** São Paulo: Memória Jurídica Editora, 178/179.

Com efeito, a cooperação internacional entre os Estados representa a melhor medida a ser adotada. A concepção de soberania precisa ser relativizada para que a lei seja efetivamente aplicada, de forma que o transgressor responda pelo crime que praticou.

5 CONSIDERAÇÕES FINAIS

É fato que a sociedade está inserida em uma intensa revolução tecnológica, marcada pelo surgimento do computador e da internet. A internet, especificamente, revolucionou a vida das pessoas, que se encontram enclausuradas no mundo digital.

Importante registrar, que a internet trouxe inúmeros benefícios à sociedade, notadamente, a simplificação da busca de informações, bem como a produção de conhecimento. A internet como meio de comunicação em massa transformou a sociedade contemporânea na sociedade da informação, responsável pelo rompimento das fronteiras territoriais.

No entanto, o uso da internet não ficou restrito a vantagens, tendo em vista que criminosos se apoderaram do sistema para perpetrar seus desígnios, fazendo surgir uma nova espécie de criminalidade: a criminalidade informática. Daí a importância da legislação penal, na tutela dos bens jurídicos da sociedade e do Estado.

Como foi tratado acima, é possível verificar que essa modalidade criminosa é muito difícil de ser reprimida, seja pela especificidade do crime, pela a ausência de lei regulamentadora ou devido a ineficiência dos órgãos investigativos.

Com efeito, a internet é um mecanismo muito interessante para os criminosos porque favorece o anonimato, o que dificulta a identificação e localização dos transgressores. Grande parte dos delitos informáticos não são punidos pela impossibilidade de rastrear e comprovar a conduta perpetrada.

Outrossim, soma-se a isso a dificuldade que se tem para atribuir a determinado país a competência para julgar os delitos informáticos transnacionais, em decorrência do pressuposto da supremacia, cuja visão clássica é patentemente retrograda e merece relativização.

A concepção classicista de soberania exprimi a ideia de que o Estado tem o poder de aplicar suas leis dentro do território que ocupa, não sendo possível a intervenção de terceiros, todavia, em razão da nova modalidade criminosa que pode violar bens jurídicos de diversos países ao mesmo tempo, essa visão deve ser relativizada.

Ressalta-se, entretanto, que a relativização mencionada não diz respeito a perda de poderes ou submissão à vontade de outros países no que se refere a

organização e atuação do Legislativo, Executivo e do Judiciário. Ela se justifica na necessidade de instrumentos jurídicos de cooperação internacional em matéria criminal, que fomentem a atuação conjunta dos países no tocante a harmonização das leis, a investigação policial e delimitação de competências.

Ora, criou-se um Tribunal Internacional para julgar crimes de genocídio, crimes contra a humanidade, crimes de guerra e os crimes de agressão, portanto, também é plenamente possível e viável a criação de leis internacionais com o objetivo de definir a competência jurisdicional das nações. Talvez a implementação de um Tribunal internacional para julgar crimes informáticos mais graves resolva o problema.

Com efeito, no âmbito interno, a repressão dos crimes informáticos esbarra da ausência de uma legislação adequada. Inúmeros delitos informáticos ainda carecem de tipificação penal, entre eles, o acesso ilegítimo, interferência de dados informáticos, interferência em sistemas e uso abusivo de dispositivos.

Não obstante, o ordenamento jurídico brasileiro até inovou em alguns aspectos conforme restou apresentado neste trabalho, todavia, as inovações não foram suficientes para proteger com eficiência os bens jurídicos da sociedade.

A Lei Carolina Dieckmann, por exemplo, foi promulgada às pressas em razão da forte tensão exercida pela mídia. O projeto inicial que deu origem a lei já tramitava no Congresso Nacional há anos, contudo, somente após uma atriz de renome ser vítima do crime informático, é que o Poder Legislativo buscou reprimi-lo.

Assim, é possível perceber que são variados os obstáculos para a repressão e prevenção dos crimes informáticos (falta de legislação específica, ausência de capacidade técnica dos órgãos investigativos e a impossibilidade de definir a competência jurisdicional).

Por conta disso, cabe aos Poderes Públicos do Brasil e das demais nações implementarem mecanismos efetivos de combate à criminalidade informática, de modo a tipificar crimes, fixar penas maiores, bem como estabelecerem regras congruentes de competência. De modo geral, a cooperação internacional representa a mais adequada forma para o combate à criminalidade, eis que o problema assola o mundo todo.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSUNÇÃO, Marco Flávio Araújo. **Segredos do Hacker Ético.** 2ª ed. Visual Books: Florianópolis, 2008, p. 13.

BATISTA, Nilo. **Introdução crítica ao direito penal brasileiro**. 11 ed. Rio de Janeiro: Revan. 2007.

BEZERRA , Arthur C.; WALTZ, Igor. **Privacidade, neutralidade e inimputabilidade da internet no Brasil,** Revista Eptic Online Vol.16 n.2.

BITENCOURT, Cezar Roberto. **Tratado de direito penal: parte especial, 2.** 10. ed. São Paulo: Saraiva, 2010.

BITENCOURT, Cezar Roberto. **Tratado de direito penal: parte geral, 1.** 15. ed. rev. atual., ampl. São Paulo: Saraiva, 2010.

BLUM, Renato Opice**. Crimes eletrônicos – a nova lei é suficiente?** Disposível em: http://www.migalhas.com.br/dePeso/16,MI172711,101048-Crimes+eletronicos+a+nova+lei+e+suficiente. Acessado em: 20 de set. 2016.

BOBBIO, Norberto. **A era dos direitos**. Tradução de Carlos Nelson Coutinho, apresentação de Censo Lafer. Nova ed. Rio de Janeiro: Elsevier, 2004, 7ª reimpressão.

BRASIL, Lei nº 12.735, de 30 de Novembro de 2012. Altera o Decreto-Lei nº 2.848, de 07 de dezembro de 1940 – Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 – Código Penal Militar, e a Lei nº 7.716, de 05 de janeiro de 1989. **Diário Oficial da República Federativa do Brasil.** Brasília, DF, 30 de nov. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm. Acesso em 10 ago. 2016.

BRASIL, Superior Tribunal de Justiça. **ALERTA: Golpe eletrônico utiliza nome do STJ para roubar dados pessoais.** Disponível em: http://www.stj.jus.br/sites/STJ/default/pt_BR/Comunica%C3%A7%C3%A3o/%C3%9Altimas-not%C3%ADcias/ALERTA:-Golpe-eletr%C3%B4nico-utiliza-nome-do-STJ-para-roubar-dados-pessoais. Acessado em: 20 de set. 2016.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil.** Brasília: Senado, 1988.

BRASIL. Lei nº 12.737, de 30 de Novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto- Lei nº 2.848, de 07 de dezembro de 1940 – Código Penal. **Diário Oficial da República Federativa do Brasil.** Brasília, DF, 30 de nov. 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 10 ago. 2016.

BRASIL. Lei nº 12.965, de 23 de Abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da República Federativa do Brasil.** Brasília, DF, 23 de abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 10 ago. 2016

BRUM, Eliane; AZEVEDO, Solange. **Suicídio.com – Sites na internet incentivam adolescentes como o gaúcho Yoñlu a se matar e ajudam a escolher o método**. Disponível em: http://revistaepoca.globo.com/Revista/Epoca/0,,EDR81603-6014,00.html, Acesso em: 20 de set. 2016.

CAPEZ, Fernando. **Curso de direito penal, volume 2, parte especial – dos crimes contra a pessoa e dos crimes contra o sentimento religioso e contra o respeito aos mortos (arts. 121 a 212)**. 10. ed. São Paulo: Saraiva, 2010.

CAPEZ, Fernando. **Curso de direito penal, volume 2, parte especial – dos crimes contra a pessoa e dos crimes contra o sentimento religioso e contra o respeito aos mortos (arts. 121 a 212)**. 10. ed. São Paulo: Saraiva, 2010.

CARVALHO, Marcelo Sávio Revoredo Menezes de. **A trajetória da internet no Brasil: do surgimento das redes de computadores à instituição dos mecanismos de governança.** 2006. 259 f. Dissertação (Mestrado em Ciências de Engenharia de Sistemas e Computação) – Programa de Pós-graduação de engenharia da Universidade Federal do Rio de Janeiro, 2006.

CASTRO, Carla Rodrigues Araújo. **Crimes de informática e seus Aspectos Processuais**. 2ª ed. Rio de Janeiro: Lumen Juris, 2003.

CASTRO, Luiz Augusto Sartori de. **“Lei Carolina Dieckmann” seria a salvação da internet?**. Disponível em: http://www.migalhas.com.br/dePeso/16,MI167980,81042-Lei+Carolina+Dieckmann+seria+a+salvacao+da+internet. Acessado em: 21 de set. 2016.

Cento de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Cartilha de segurança para internet.** Disponível em: http://cartilha.cert.br/ataques/. Acessado em 20 de set. 2016.

CONTE, Christiany Pegorari. **Jurisdição e competência nos crimes informáticos.** Revista Brasileira de Meio Ambiente Digital e Sociedade da Informação. V. 01, nº. 01, p. 49-208, 2014.

COSTA, Fernando José da. ***Locus Delicti* nos crimes informáticos.** 2011. 355 f. Tese (Doutorado em Direito) – Faculdade de Direito da USP, São Paulo, 2011.

CUNHA, Rogério Sanches. **Manual de direito penal – parte especial (arts. 121 ao 361).** 8 ed. rev. ampl. e atual. Salvador/BA: JusPODIVM, 2016.

CUNHA, Rogério Sanches. **Manual de direito penal – parte geral (arts. 1º ao 120).** 3 ed. rev. ampl. e atual. Salvador/BA: JusPODIVM, 2015.

Delegado. G1-Tecnologia, 06 jan. 2011. Disponível em: http://g1.globo.com/tecnologia/noticia/2011/01/trabalho-contra-crimes-virtuais-ainda-esta-longe-do-ideal-diz-delegado.html. Acessado em 21 de set. 2016.

FABEL, Evandro. **Polícia Civil investiga possível incentivo ao suicídio no Orkut.** Disponível em: http://www.gazetadigital.com.br/conteudo/show/secao/4/materia/138370. Acesso em: 20 de set. 2016.

FERREIRA LIMA, Paulo Marco. **Bem jurídico e os crimes de computador**. Revista Justitia, São Paulo, V. 197, p. 381-385, jul/dez. 2007.

FERREIRA, Ivette Senise. **A criminalidade informática**. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto (coord.). **Direito e internet: aspectos jurídicos relevantes**. Bauru: Edipro, 2000. p. 207 – 237.

FRAGOSO, Heleno Cláudio. **Lições de direito penal: parte especial: arts. 121 a 212 do CP.** Rio de Janeiro: Forense, 1983.

GIMESES, Amanuel Alberto Sperandio Garcia. **Crimes virtuais**. Disponível em: http://bdjur.stj.jus.br/dspace/handle/2011/64929, acesso em: 20 de ago. de 2016.

GÓIS JÚNIOR, José Caldas. **O direito na era das redes: a liberdade e o delito no ciberespaço**. Bauru/SP: EDIPRO, 2001, p. 120. *Apud:* COSTA, Fernando José da. ***Locus Delicti* nos crimes informáticos.** 2011. 355 f. Tese (Doutorado em Direito) – Faculdade de Direito da USP, São Paulo, 2011.

GOUVÊA, Sandra. **O direito na era digital: crimes praticados por meio da informática.** Rio de Janeiro: Mauad, 1997.

GRECO FILHO, Vicente. **Algumas observações sobre o direito penal e a Internet**. Boletim IBCCRIM, ano 8, nº. 95, out. 2000.

GRECO, Rogério. **Curso de direito penal – parte especial, volume II: introdução à teoria geral da parte especial: crimes contra a pessoa**. 11 ed. rev. e atual. Rio de Janeiro: Impetus, 2015.

GRECO, Rogério. **Curso de direito penal – parte geral**. 18 ed. rev. ampl. e atual. Rio de Janeiro: Impetus, 2016.

HUNGRIA, Nélson, FRAGOSO, Heleno Cláudio. **Comentários ao código penal,** v.1, tomo 1: arts. 1º ao 10º. 5 ed. Rio de Janeiro: Forense, 1976.

HUNGRIA, Nélson, FRAGOSO, Heleno Cláudio. **Comentários ao código penal,** v.5, arts. 121 ao 136. 5 ed. Rio de Janeiro: Forense, 1979.

HUNGRIA, Nélson, FRAGOSO, Heleno Cláudio. **Comentários ao código penal,** v.6, arts. 137 ao 154. 5 ed. Rio de Janeiro: Forense, 1980.

HUNGRIA, Nélson, FRAGOSO, Heleno Cláudio. **Comentários ao código penal,** v.7, arts. 155 ao 196. 1. ed. Rio de Janeiro: Forense, 1955.

HÚNGRIA. **Convenção sobre o Cibercrime**. Disponível em: http://www.internacional.mpf.mp.br/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf. Acessado em 20 de set. 2016.

LIMA, Paulo Marco Ferreira. **Crimes de computador e segurança computacional**, Campinas, São Paulo: Millennium, 2005.

MASSON, Cleber Rogério. **Direito penal esquematizado – parte geral – vol. 1.** 4ª. ed. rev., atual. e ampl. São Paulo: Método, 2011.

MASSON, Cleber. **Direito penal esquematizado: parte especial – vol. 2**. 7ª. ed. rev., atual. e ampl. Rio de Janeiro: Forense; São Paulo: MÉTODO, 2015.

MATTELART, Armand. **A era da informação: gênese de uma denominação descontrolada.** Tradução de Francisco Rüdiger. Revista FAMECOS, Porto Alegre, V. 08, nº. 15, p. 07-23, ago. 2001.

MONTEIRO NETO, João Araújo. **Aspectos constitucionais e legais do crime eletrônico.** 2008. 191 f. Dissertação (Mestrado em Direito Constitucional), Universidade de Fortaleza, 2008.

MORAIS NETO, Arnaldo Sobrinho de. **Crimes e cooperação penal internacional: um enfoque à luz da convenção de Budapeste.** 2009,. 188 f. Dissertação (Mestrado em Direito) – Universidade Federal da Paraíba - UFPB, João Pessoa/PB, 2009.

NETO, Mário Furlaneto, GUIMARÃES, José Augusto Chaves. **Crimes na internet: elementos para uma reflexão sobre a ética informacional.** Periódico do Conselho da Justiça Federal, Brasília, V. 07, nº. 20, p. 67-73, jan./mar. 2003.

NOGUEIRA, Sandro D'Amato. **Crimes de informática.** São Paulo: BH Editora, 2008.

NUCCI, Guilherme de Souza. **Código penal comentado**. 10. ed. rev., atual. e ampl. São Paulo: Editora Revista dos Tribunais, 2010.

NUCCI, Guilherme de Souza. **Manual de direito penal**. 7 ed. rev., atual. e ampl. Rio de Janeiro: Revista dos Tribunais, 2011.

OLIVEIRA, Carlos Eduardo Elias de. **Aspectos Principais da Lei nº 12.965, de 2014, o Marco Civil da Internet: subsídios à comunidade jurídica**. Brasília: Núcleo de Estudos e Pesquisas/CONLEG/ Senado, abr./2014.

OLIVEIRA, Diego Bianchi de; SILVA, Ricardo Guilherme Silveira Corrêa. **O viés digital do suicídio: instigação, induzimento e auxílio ao suicídio em ambientes virtuais.** In: XXIV CONGRESSO NACIONAL DO CONPEDI – UFMG/FUMEC/Dom Helder Câmara, 2015, Florianópolis, Direito Penal e Constituição, Florianópolis/MG, 2015, p. 563-581.

PAESANI, Lilian Minardi. **Direito e Internet: liberdade de informação, privacidade e responsabilidade civil.** 6. ed. São Paulo: Atlas, 2013.

PINHEIRO, Reginaldo César. **Os Crimes Virtuais na esfera jurídica brasileira**. **Boletim IBCCrim.** Ano 8, n 101, abril/2001.

PRADO, Luiz Regis. **Curso de direito penal brasileiro – vol. 1 - parte geral: arts. 1º ao 120.** 9 ed. rev. atual. e ampl. São Paulo: Revistas dos Tribunais. 2010.

ROHR, Altieres. **Brasil lidera ranking de usuários atacados por phishing, diz Kaspersky Lab**. Disponível em: http://g1.globo.com/tecnologia/blog/seguranca-digital/post/brasil-lidera-ranking-de-usuarios-atacados-por-phishing-diz-kaspersky-lab.html. Acessado em 20 de set. 2016.

ROHR, Altieres. **Trabalho Contra Crimes Virtuais Ainda Está Longe do Ideal, Diz**
ROQUE, Sérgio Roque. **Criminalidade Informática – Crimes e Criminosos do Computador.** 1 ed. São Paulo: ADPESP Cultural, 2007.

ROSSINI, Augusto Eduardo de Souza. **Informática, Telemática e Direito Penal.** São Paulo: Memória Jurídica Editora, 2004.

SANT'ANNA, Ivan. **Plano de Ataque: a história dos vôos de 11 de setembro.** Rio de Janeiro: Objetiva, 2006.

SANTOS, Coriolano Aurélio de Almeida Camargo; FRAGA, Ewelyn Schots. **As Múltiplas Faces dos Crimes Eletrônicos e dos Fenômenos Tecnológicos e Seus Reflexos no Universo Jurídico.** São Paulo: OAB SP, 2010.

SILVA, Alessandra Mara de Freitas; SILVA, Cristian Kiefer da. **O problema da tipificação dos crimes informáticos: aspectos controversos a respeito da aplicação do artigo 154-a da lei nº 12.737/2012 "Lei Carolina Dieckmann".** Disponível em: http://www.publicadireito.com.br/artigos/?cod=2a5b63fbaadcaa8c. Acessado em: 20 de set. 2016.

THOMPSON, Marcelo, **Marco civil ou demarcação de direitos? Democracia, razoabilidade e as fendas na internet do Brasil,** rda – revista de Direito Administrativo, Rio de Janeiro, v. 261, p. 203-251, set./dez. 2012.

TORRE, Marina Giantomassi Della. **Aspectos processuais e penais dos crimes de computador.** 2009. 183 f. Dissertação (Mestrado em Direito Processual Penal), São Paulo, 2009.

VALIN, Celso. **A questão da jurisdição e da territorialidade nos crimes praticados pela internet.** *In:* ROVER, Aires José (organizador). **Direito, sociedade e informática: limites e perspectivas da vida digital.** Florianópolis: Fundação Boiteux, 2000.

VIANNA, Túlio Lima. **Do acesso não autorizado a sistemas computacionais: fundamentos de direito penal informático.** 2001. 241 f. Dissertação (Mestrado em Direito) – Faculdade de Direito da UFMG, Belo Horizonte, 2001.

WENDT, Emerson, JORGE, Higor Vinicius Nogiueira. **Crimes cibernéticos: ameaças e procedimentos de investigação.** 2. ed. Rio de Janeiro: Brasport, 2013.

WOLTON, Dominique. **Pensar a internet.** Tradução de Daniela Dariano. Revista FAMECOS, Porto Alegre, V. 08, nº. 15, p. 24-28, ago. 2001.

ZAFFARONI, Eugênio Raúl, PIERANGELI, José Henrique. **Manual de direito penal brasileiro: volume 01: parte geral.** 9. ed. rev. e atual. São Paulo: Editora Revista dos Tribunais, 2011.