UNIVERSIDADE PRESBITERIANA MACKENZIE
FACULDADE DE DIREITO

ALESSANDRA NAVARRO HAMID

CIBERCRIMINALIDADE:
ASPECTOS VITIMOLÓGICOS SOBRE OS DELITOS INFORMÁTICOS

SÃO PAULO
2021

ALESSANDRA NAVARRO HAMID

CIBERCRIMINALIDADE:
ASPECTOS VITIMOLÓGICOS SOBRE OS DELITOS INFORMÁTICOS

Trabalho de Conclusão de Curso apresentado à Faculdade de Direito da Universidade Presbiteriana Mackenzie como requisito parcial para obtenção do grau de Bacharel em Direito.

Orientadora: Profª Dra. Thamara Duarte Cunha Medeiros

SÃO PAULO
2021

CIBERCRIMINALIDADE:
ASPECTOS VITIMOLÓGICOS SOBRE OS DELITOS INFORMÁTICOS

Trabalho de Conclusão de Curso apresentado à Faculdade de Direito da Universidade Presbiteriana Mackenzie como requisito parcial para obtenção do grau de Bacharel em Direito.

Aprovada em ____/____/____

Banca examinadora

_____
Profª Dra. Thamara Duarte Cunha Medeiros
Universidade Presbiteriana Mackenzie

_____
Profª Dra. Márcia Cristiana de Souza Alvim
Universidade Presbiteriana Mackenzie

_____
Profª Dra. Renata da Rocha
Universidade Presbiteriana Mackenzie

À minha família, meu bem mais precioso, por serem minha base, por todo amor e carinho.

À minha mãe, Roseli, por ter me ensinado desde cedo a importância do estudo, por toda a sua dedicação, perseverança, atenção e cuidado, saiba que a senhora é a mulher mais forte que eu já conheci.

À minha irmã Lhais, meu espelho como pessoa e profissional, por todo incentivo, por ser essa pessoa extraordinária.

AGRADECIMENTOS

À minha orientadora, Dra. Thamara Duarte Cunha Medeiros, pela atenção e direção, sem ela não seria possível a conclusão deste trabalho.

A todos aqueles que contribuíram de alguma forma para que eu chegasse até aqui.

CIBERCRIMINALIDADE:
ASPECTOS VITIMOLÓGICOS SOBRE OS DELITOS INFORMÁTICOS

ALESSANDRA NAVARRO HAMID

Resumo: O presente artigo descreve aspectos jurídicos na área penal advindos do avanço tecnológico e do uso da internet, bem como, apresenta noções gerais de cibercriminalidade. Para sua realização foi utilizado o método analítico e descritivo por meio de pesquisa bibliográfica em artigos científicos, doutrinas e notícias jornalísticas. O enfoque desta pesquisa é o estudo da vítima do delito informativo sob a ótica da vitimologia, assim como, aborda aspectos comportamentais do usuário da internet que o colocam sob risco de eventuais danos e facilitam a cibervitimização, levando em consideração a premissa de que a postura do usuário no ciberespaço é muito significativa para sua própria proteção. Por fim, serão apresentadas possíveis formas de prevenção de delitos informáticos.

Palavras-chave: Cibercriminalidade. Vítima. Cibervitimização. Delitos informáticos. Internet.

CYBERCRIMINALITY:
VICTIMOLOGICAL ASPECTS ON COMPUTER-RELATED CRIMES

Abstract: The present article describes legal aspects in the criminal area arising from technological advances and the use of the internet, as well as presents general notions of cybercrime. For its realization, the analytical and descriptive method was used through bibliographical research in scientific articles, doctrines and journalistic news. The focus of this research is the study of the victim of informative crime under the viewpoint of victimology, as well as, approaches behavioral aspects of the internet user that put him at risk of eventual damage and facilitate cyber victimization, taking into consideration the premise that the user's posture in cyberspace is very significant for his own protection. Finally, possible ways of preventing computer-related crimes will be presented.

Keywords: Cybercrime. Victim. Cyber victimization. Computer-related crimes. Internet.

INTRODUÇÃO

O progresso no fenômeno da globalização nos apresentou a internet, que revolucionou o mundo e as comunicações, de forma inimaginável. Nesse sentido, a internet tornou o mundo mais próximo, suprimindo a distância geográfica, derrubando barreiras de uma forma tão grande, que hoje é possível conhecer lugares e pessoas de toda parte, sem sair de sua casa. A internet invadiu a vida cotidiana e nos fez dependentes.

Essa rede mundial democratizou o acesso ao conhecimento, tornou-se um mecanismo de disseminação de informação, permitindo acesso fácil às informações. A criação do jornal impresso, do telégrafo, do rádio, da televisão e do telefone, não foram tão contundentes e transformadoras quanto a internet. Trata-se de fenômeno da universalização das comunicações.

A Organização das Nações Unidas (ONU), em 2016, publicou um relatório sobre a Liberdade de Opinião e Expressão[1], se manifestando no sentido de que o acesso à internet é um direito humano e universal. Além disso, desconectar a população da web é um crime e uma violação aos direitos humanos.

Hoje, o Brasil é o quarto país em número de usuários de internet no mundo, com aproximadamente 130 milhões de pessoas conectadas à rede [2], cerca de 70 por cento da população do país. Com o crescente número de usuários da internet, o número de delitos informáticos cresceu absurdamente. Dados de notificações recebidas pela Central Nacional de Denúncias de Crimes Cibernéticos, uma parceria da ONG Safernet Brasil com o Ministério Público Federal (MPF), revelam que de janeiro a dezembro de 2020, foram registradas 156.692 denúncias anônimas, contra 75.428 em 2019 [3], ou seja, as denúncias dobraram. As denúncias que lideram o ranking são relativas aos crimes de pornografia infantil, neonazismo, racismo, violência ou discriminação contra a mulher.

---

[1] Relatório da ONU declara internet como um direito humano. Tecnologia Terra. Disponível em: <http://tecnologia.terra.com.br/internet/relatorio-da-onu-declara-internet-como-um-direito-humano,8ea9dceae77ea310VgnCLD200000bbcceb0aRCRD.html>. Acesso em: 15 de março de 2021.

[2] TIC Domicílios 2019 (**Cetic**.br) Disponível em: <https://cetic.br/media/analises/tic_domicilios_2019_coletiva_imprensa.pdf>. Acesso em: 15 de março de 2021.

[3] Denúncias de crimes cometidos pela internet mais que dobram em 2020. G1 Globo. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2021/02/09/numero-de-denuncias-de-crimes-cometidos-pela-internet-mais-que-dobra-em-2020.ghtml>. Acesso em: 15 de março de 2021.

A cada dia surgem novos fatos e novas relações que necessitam da tutela do Direito. Nessa avalanche de novas transformações geradas pela informática, o direito também observou reflexos dessas transformações em seus ramos, e assim, deve se adequar à nova realidade do mundo digital. Inevitavelmente, o ciberespaço abriu caminho para a possibilidade de aperfeiçoamento de crimes tradicionais.

O presente trabalho tem como objetivo investigar os problemas jurídicos na área penal advindos do avanço tecnológico e do uso da internet, bem como, estudar essa nova espécie de delito, os pontos relevantes do Direito Penal Informático. Além disso, aborda aspectos vitimológicos do delito informático, a vítima desse tipo delituoso e suas especificidades, e o autor do delito no ambiente digital.

Para sua realização foi utilizado o método analítico e descritivo por meio de pesquisa bibliográfica em artigos científicos, doutrinas e notícias jornalísticas.

O primeiro capítulo, é dedicado a apresentação da revolucionária rede mundial de computadores. Trazendo os pontos mais importantes: o surgimento e a consolidação da rede. Desde a criação de um sistema de transmissão de dados, que não era chamado de internet, até a chegada ao Brasil, a fim de trazer uma melhor compreensão desse fenômeno que é a internet.

O segundo capítulo, possui um viés descritivo de aspectos penais do direito penal informático, apresenta aspectos sobre competência para legislar sobre direito penal informático e sobre a competência jurisdicional nos crimes Informáticos, bem como, aborda o conceito de delito penal informático, classificações doutrinárias, os sujeitos ativo e passivo dessa nova modalidade de delito.

Em seguida, o terceiro e último capítulo aborda a ciência chamada criminologia e seu ramo de vitimologia. Trata também da necessidade de uma criminologia específica para estudar os ciber delitos, e por fim, há um item dedicado à prevenção dos delitos informáticos.

1. A REDE MUNDIAL DE COMPUTADORES - INTERNET

Abordaremos neste capítulo a rede mundial de computadores. Trazendo os pontos mais importantes: o surgimento e a consolidação da rede. Desde a criação de um sistema de transmissão de dados, que não era chamado de internet, até a chegada ao Brasil.

1.1 O SURGIMENTO DA INTERNET

A internet ou rede mundial de computadores, diferente do que conhecemos hoje, foi criada durante o contexto da Guerra Fria, na década de 1960, resultado de pesquisas militares do governo norte americano. Nesse período, marcado por forte oposição ideológica e política, qualquer inovação que os Estados Unidos ou a União Soviética promovessem, tinha grande importância e poderia influenciar nessa disputa.

A proposta inicial era criar uma ferramenta de comunicação militar, que protegesse as informações sigilosas de possíveis ataques russos, mesmo que outros meios de telecomunicações fossem destruídos. Assim, surgiu a ARPAnet (Advanced Research Projects Agency Network), que operava através de um sistema de transmissão de dados em rede de computadores. A informação, antes de ser enviada, é dividida em pequenas partes ou pacotes, essa técnica é chamada de chaveamento de pacotes[4].

A primeira conexão da ARPANET ocorreu em 29 de outubro de 1969, entre a Universidade da Califórnia em Los Angeles (UCLA), e o Instituto de Pesquisa de Stanford[5]. A princípio ligando quatro computadores, mais tarde outros computadores de universidades e centros de pesquisa se conectaram. Nos anos 80, a utilização do

---

[4] CARVALHO, Marcelo Sávio Revoredo Menezes de. A trajetória da Internet no Brasil: do surgimento das redes de computadores à instituição dos mecanismos de governança. [Rio de Janeiro] 2006, p. 11. Disponível em: <https://www.cos.ufrj.br/uploadfile/1430748034.pdf>. Acesso em 15 de março de 2021.

[5] Mãe da internet faz 50 anos, conheça a história da ARPANET. Olhar Digital. Disponível em: <https://olhardigital.com.br/2019/10/24/noticias/mae-da-internet-faz-50-anos-conarpanetheca-a-historia-da-/ >. Acesso em: 16 de março de 2021.

TCP/IP (Transmission Control Protocol/Internet Protocol), possibilitou a conexão e integração de redes diferentes, em maior escala[6].

Em 1989, foi criada a World Wide Web - Rede Mundial de Computadores, conhecida como WWW ou Web, pelo pesquisador britânico Tim Berners-Lee, sendo lançada em 1992,[7] no Laboratório Europeu de Física de Partículas (CERN), conquistando milhares de usuários pela versatilidade. Trata-se de um sistema de documentos em hipermídia que são interligados e executados na Internet, denominados hipertextos, que são textos exibidos em formato digital, os quais podem conter informações em formato de imagens, sons, vídeos etc. O acesso a tais informações se dá por meio de links, que servem como uma ponte entre os mais diversos sites da Internet e seus conteúdos.

Nos anos 90, a ARPAnet foi transformada em NSFnet (National Science Foundation's Network), possibilitando a interconexão de diferentes universidades, e institutos de pesquisas pelo mundo e os computadores da ARPANET[8].

Assim, a internet, então restrita às universidades e centros de pesquisa, começou a se popularizar a partir dos anos 90, e cresceu em proporções gigantescas. Então, a ferramenta criada no contexto de guerra tornou- se parte fundamental no dia a dia das pessoas em todo mundo.

Hoje em dia é quase impossível imaginar um mundo sem internet, quem nunca passou um dia sem acesso e se sentiu perdido, ou, teve atrasos em seu trabalho e estudos, não há dúvida que somos extremamente dependentes dessa rede. A internet não trouxe apenas benefícios, mas também espaço para condutas criminosas.

---

[6] FERNANDEZ, Marcial Porto. Rede de Computadores. Ceará. Ed. UECE. 2015. Disponível em: <http://www.uece.br/computacaoead/index.php/downloads/doc_download/2100redescomputadores>. Acesso em: 16 de março de 2021.

[7] A World Wide Web completa 25 anos. Em 12 de março de 1989 o britânico Tim Berners-Lee descreveu o protocolo de transferências de hipertextos. El País. Disponível em:<https://brasil.elpais.com/brasil/2014/03/11/tecnologia/1394554623_973239.html#:~:text=Em%2012%20de%20mar%C3%A7o%20de,protocolo%20de%20transfer%C3%AAncias%20de%20hipertextos&text=Em%2012%20de%20mar%C3%A7o%20de%201989%2C%20o%20pesquisador%20brit%C3%A2nico%20Tim,seria%20a%20World%20Wide%20Web>. Acesso em: 16 de março de 2021.

[8] Monteiro, Luís. A internet como meio de comunicação: possibilidades e limitações s. 2001, p.28. Disponível em: <http://www.portcom.intercom.org.br/pdfs/621005553999492233255344810859412805 73.pdf>. Acesso em: 17 de março de 2021.

1.2 A INTERNET NO BRASIL

A internet chega ao Brasil em 1987, com uso estritamente acadêmico e científico, a princípio, a FAPESP (Fundação de Amparo à Pesquisa do Estado de São Paulo) e o LNCC (Laboratório Nacional de Computação Científica), conectaram-se a instituições nos EUA[9]. Após, em 1988, a Universidade Federal do Rio de Janeiro conectou-se à Universidade da Califórnia em Los Angeles.

Pensando nos benefícios que essa tecnologia poderia trazer ao meio acadêmico, em 1989, o Ministério da Ciência e Tecnologia (MCT), criou a Rede Nacional de Pesquisa (RNP), um projeto cujo objetivo era desenvolver uma moderna infraestrutura nacional de rede de internet e promover a disseminação do uso da internet no país, com finalidade educacional e social[10]. Em 1992, foi implementada a “espinha dorsal” de comunicação, um backbone nacional, com a velocidade mínima de 9.600 bits por segundo (bps)[11], resultado de um conjunto de conexões interestaduais, ligando dez estados e o Distrito Federal.

O Ministério das Comunicações (MC), aliado ao Ministério da Ciência e Tecnologia (MCT), decidiram expandir a rede de internet, criando o backbone nacional de uso misto, a rede acadêmica foi ampliada para uso comercial. Em maio de 1995, foi criado o Comitê Gestor da Internet no Brasil, com a participação do MC e do MCT, de entidades operadoras e gestoras de espinhas dorsais, de representantes de provedores de acesso ou de informações, de representantes de usuários e da comunidade acadêmica[12]. O Comitê era responsável por coordenar, reunir e integrar as iniciativas ligadas ao uso e desenvolvimento de serviços de internet, como também, indicar padrões e procedimentos técnicos e operacionais, organizar a atribuição de endereços, e o registro de nomes de domínios.

---

[9] História da internet no Brasil. Disponível em: <https://homepages.dcc.ufmg.br/~mlbc/cursos/internet/historia/Brasil.html>. Acesso em: 17 de março de 2021.

[10] Rede Nacional de Ensino e Pesquisa. Nossa história. Disponível em: <https://www.rnp.br/sobre/nossa-história>. Acesso em: 17 de março de 2021.

[11] História da internet no Brasil. Disponível em: <https://homepages.dcc.ufmg.br/~mlbc/cursos/internet/historia/Brasil.html>. Acesso em: 17 de março de 2021.

[12] História da internet no Brasil. Disponível em: <https://homepages.dcc.ufmg.br/~mlbc/cursos/internet/historia/Brasil.html>. Acesso em: 19 de março de 2021.

A Nota Conjunta do Ministério da Ciência e Tecnologia e Ministério das Comunicações, de maio de 1995, foi responsável pela abertura da rede, ampliando o acesso para operação comercial da rede, criando o provedor de acesso privado. É possível extrair da nota[13]:

> 1.1 O Governo considera de importância estratégica para o País tornar a Internet disponível a toda a Sociedade, com vistas à inserção do Brasil na Era da Informação.
> 1.2 O provimento de serviços comerciais Internet ao público em geral deve ser realizado, preferencialmente, pela iniciativa privada.
> 1.3 O Governo estimulará o surgimento no País de provedores privados de serviços Internet, de portes variados, ofertando ampla gama de opções e facilidades, visando ao atendimento das necessidades dos diversos segmentos da Sociedade.
> 1.4 A participação das empresas e órgãos públicos no provimento de serviços Internet dar-se-á de forma complementar à participação da iniciativa privada, e limitar-se-á às situações onde seja necessária a presença do setor público para estimular ou induzir o surgimento de provedores e usuários.

Assim, o governo optou por deixar a exploração dos serviços comerciais Internet ao público em geral, para ser realizada pela iniciativa privada, bem como determinou que a participação das empresas e órgãos públicos no provimento de serviços Internet deveria se dar de forma complementar à participação da iniciativa privada, e limitada às situações em que necessária a presença do setor público para estimular ou induzir o surgimento de provedores e usuários.

A supracitada Nota Conjunta, de 1995, definiu a internet como:

> 2.1 A Internet é um conjunto de redes interligadas, de abrangência mundial. Através da Internet estão disponíveis serviços como correio eletrônico, transferência de arquivos, acesso remoto a computadores, acesso a bases de dados e diversos tipos de serviços de informação, cobrindo praticamente todas as áreas de interesse da Sociedade.

Portanto, a internet é um conjunto de redes interligadas de computadores, que tem como objetivo fornecer ao usuário o acesso a diversos serviços de informação e comunicação.

---

[13] Nota conjunta do Ministério da Ciência e Tecnologia e Ministério das Comunicações (maio de 1995). Disponível em: <https://www.cgi.br/legislacao/notas/nota-conjunta-mct-mc-maio-1995#:~:text=1.1%20O%20Governo%20considera%20de,%2C%20preferencialmente%2C%20pela%20iniciativa%20privada>. Acesso em: 19 de março de 2021.

A imagem 1 ilustra o backbone da RNP, após a abertura da rede, em 1996:

Figura 1: Backbone da RNP em Santa Catarina no ano 1996.

Fonte: (Arquivo Histórico)[14].

Hoje em dia, o país tem muitas colunas de backbones que interconectam todos os estados do país, bem como várias conexões com outros países.

1.3 O DIREITO AO ACESSO À REDE MUNDIAL DE COMPUTADORES

A Organização das Nações Unidas (ONU), publicou um relatório sobre a Liberdade de Opinião e Expressão[15], se manifestando no sentido de que o acesso à internet é um direito humano e universal.

Além disso, desconectar a população da web é um crime e uma violação aos direitos humanos, assim, todo indivíduo tem direito à liberdade de opinião e expressão, e ao acesso à informação, segundo a ONU, nenhum Estado tem o direito de bloquear por completo o acesso à internet. De acordo com a organização,

[14] Backbone da RNP em Santa Catarina no ano 1996 (Arquivo Histórico). Memória da internet acadêmica em Santa Catarina. Disponível em: <https://memoria.pop-sc.rnp.br/backbone_rnp_1996/>. Acesso em: 19 de março de 2021.

[15] Relatório da ONU declara internet como um direito humano. Tecnologia Terra. Disponível em: <http://tecnologia.terra.com.br/internet/relatorio-da-onu-declara-internet-como-um-direito-humano,8ea9dceae77ea310VgnCLD200000bbcceb0aRCRD.html>. Acesso em: 15 de março de 2021.

a supressão desse direito viola o artigo 19, parágrafo 3°, do Pacto Internacional de Direitos Civis e Políticos, de 1966[16].

A Convenção de Budapeste sobre Crimes Cibernéticos[17], de 2001, é um instrumento internacional vinculante sobre esse tema, que tipifica a criminalidade no ciberespaço, com o objetivo de proteger a sociedade e fortalecer a cooperação internacional. Dentro dos crimes cibernéticos tipificados estão as violações a direitos autorais, fraudes de sistemas e dados, pornografia infantil e violações à segurança de redes praticados na internet.

Importante destacar, que a Convenção de Budapeste, ou Convenção sobre Cibercrime, tipifica as condutas criminosas praticadas no âmbito da internet, englobando somente os fatos típicos ocorridos especificamente no ciberespaço.

Os Estados não os únicos a violaram esse direito tão importante, a sociedade sofre de outros males, como pessoas mal-intencionadas, criminosos, e crackers, que possuem grande habilidade tecnológica, e podem não apenas violar a segurança do dispositivo de um indivíduo, mas de milhares ao mesmo tempo, como também de instituições governamentais, que nos últimos anos sofreram ataques em todo mundo.

1.4 O DIREITO AO ACESSO À REDE MUNDIAL DE COMPUTADORES NO BRASIL

A Lei n° 12.965/2014[18], conhecida como Marco Civil da Internet, é a lei que regula o uso da Internet no Brasil através de princípios, garantias, direitos e deveres para os provedores e internautas, bem como da determinação de diretrizes para a atuação do Estado.

---

[16]Pacto Internacional de Direitos Civis e Político. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm>. Acesso em: 25 de março de 2021.

[17]Convenção de Budapeste sobre Crimes Cibernéticos. Disponível em: <http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf >. Acesso em: 25 de março de 2021.

[18]Marco Civil da Internet, Lei n° 12.965/14, Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm >. Acesso em: 27 de março de 2021.

A Lei 12.965/14, conta com trinta e dois artigos, divididos em cinco capítulos. Traz um rol extenso de direitos e garantias dos usuários, estabelece princípios e deveres para o uso da Internet no Brasil, além de definições próprias dos Sistemas de Informações. O artigo 5° prevê que todo cidadão tem direito ao acesso à internet, vejamos:

> Art. 4º A disciplina do uso da internet no Brasil tem por objetivo a promoção:
> I - do direito de acesso à internet a todos;
> II - do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos;
> III - da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; e
> IV - da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados.

Assim, o direito ao acesso à internet ganha novo patamar, trata-se de direito universal e essencial ao exercício da cidadania, os usuários são assegurados de muitos direitos, inclusive o legislador fez questão de especificá-los no artigo 7° da referida lei:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
> II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
> III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
> IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;
> V - manutenção da qualidade contratada da conexão à internet;
> VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;
> VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
> VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
> a) justifiquem sua coleta;
> b) não sejam vedadas pela legislação; e
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
> IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
> X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da

> relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;
> XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;
> XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e
> XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.

O direito à inviolabilidade da intimidade e da vida privada, e o sigilo das comunicações, são garantias fundamentais protegidas pelo texto constitucional, que foram trazidas ao Marco Civil, a fim de garantir maior proteção ao indivíduo que acessa à rede. Todavia, sabemos que não foi o bastante, e o Brasil de ações significativas de proteção ao usuário da rede.

2. DIREITO PENAL INFORMÁTICO

Nos ensinamentos de Damásio de Jesus (2011, p. 45), o direito surge das necessidades humanas fundamentais, assim vejamos:

> O fato social é sempre o ponto de partida na formação da noção de Direito. O Direito surge das necessidades fundamentais das sociedades humanas, que são reguladas por ele como condição essencial à sua própria sobrevivência. É no Direito que encontramos a segurança das condições inerentes à vida humana, determinada pelas normas que formam a ordem jurídica.

O Direito Penal é um ramo do Direito Público. Segundo Fernando Capez (2011, p. 19):

> O Direito Penal é o segmento do ordenamento jurídico que detém a função de selecionar os comportamentos humanos mais graves e perniciosos à coletividade, capazes de colocar em risco valores fundamentais para a convivência social, e descrevê-los como infrações penais, cominando-lhes, em consequência, as respectivas sanções, além de estabelecer todas as regras complementares e gerais necessárias à sua correta e justa aplicação.

Por sua vez, o direito penal informático é um ramo do direito penal, logo, é também um ramo do direito público. Os crimes informáticos estão previstos na parte especial do Código Penal, mas são crimes que podem ser processados tanto

na Justiça Comum Estadual e na Justiça Comum Federal, dependendo do tipo de ilícito.

O Direito Informático, segundo o Professor Spencer Toth Sydow (2021, p. 246), têm caráter transbordante, temos um direito unilateral/unifacetado tratando de questões multilaterais/multifacetadas.

No Brasil, apenas o Marco Civil[19] e a Lei Carolina Dieckmann[20] são responsáveis pela resolução das demandas virtuais, o que, aliás, não é suficiente para resolver os conflitos que surgem na Internet nas áreas cível e penal, até que Brasil crie leis e adira a um tratado internacional mais abrangente.

2.1 COMPETÊNCIA PARA LEGISLAR SOBRE DIREITO PENAL INFORMÁTICO

O princípio da legalidade, é um dos princípios mais importantes no Direito Constitucional, é a essência do Estado de Direito, protege o cidadão de abusos do Estado. A Constituição Federal consagrou esse princípio no artigo 5°, inciso II, *“ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei”*[21]. Assim, o Estado só pode exigir condutas e comportamentos expressamente previstos em lei, e o ente estatal pode fazer apenas aquilo que a lei o permite.

Tal princípio, combinado ao princípio da anterioridade, previsto na Constituição Federal, no artigo 5°, inciso XXXIX[22], e no artigo 1°, do Código Penal[23], *“Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação*

---

[19] Marco Civil da Internet, Lei n° 12.965/14. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato 20 11-2014/2014/lei/l12965.htm>. Acesso em: 02 de abril de 2021.
[20] Lei Carolina Dieckmann, Lei n° 12.737/2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 02 de abril de 2021.
[21]Constituição Federal. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 06 de abril de 2021.
[22]Constituição Federal. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 06 de abril de 2021.
[23]Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 06 de abril de 2021.

legal", são peças fundamentais ao Direito Penal, e seu ramo, Direito Penal Informático.

A competência para legislar sobre Direito Penal é competência privativa da União e encontra-se no artigo 22, inciso I, da Carta Magna[24]. Logo, a união também será competente para legislar sobre Direito Penal Informático.

> Art. 22. Compete privativamente à União legislar sobre:
>
> I - Direito civil, comercial, penal, processual, eleitoral, agrário, marítimo, aeronáutico, espacial e do trabalho;

Quanto à iniciativa, de acordo com o artigo 61, da CF, podem propor a iniciativa para a criação de leis em matéria penal: a) os membros do Congresso Nacional (art. 61, caput, CF); b) o Presidente da República (art. 61, caput, CF); c) os cidadãos por meios de iniciativa popular através da apresentação à Câmara dos Deputados de projeto de lei (art. 61, § 2º CF)[25].

2.2 CONCEITUAÇÃO DO DELITO PENAL INFORMÁTICO

Na literatura contemporânea, há várias definições para essa espécie de delito: "crime cibernético", "crime informático", "e-crime", "cibercrime", "crime eletrônico", "delinquência informática" ou "crime digital". Todos são termos aplicáveis à atividade delitiva que tem como objeto ou faz uso de um computador, uma rede de computadores ou apenas um dispositivo conectado à rede.

O termo "cibercrime" foi criado em Lyon, na França, nos anos 90, após uma reunião de um subgrupo das nações do G8, que discutiu os crimes realizados por aparelhos eletrônicos ou mediante a disseminação de informações pela internet[26]. O termo foi usado para descrever, de forma ampla, todos os tipos de crime praticados

---

[24]Constituição Federal. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 07 de abril de 2021

[25]Constituição Federal. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 07 de abril de 2021

[26] BARBAI. M.A. A criminalidade no espaço digital; a formulação do sentido. In. DIAS, Cristiane. Formas de mobilidade no espaço e-urbano: sentido e materialidade digital [online]. (Serie e-urbano, v.2), 2013. Disponível em: <https://www.labeurb.unicamp.br/livroEurbano/>. Acesso em: 10 de abril de 2021.

na Internet ou nas novas redes de telecomunicações, que na década de 90 se tornavam cada vez mais acessíveis a um grande número de usuários.

O secretário executivo da Associação de Direito e Informática do Chile, Claudio Líbano Manzur, define crimes cibernéticos como sendo:

> Todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una série de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la victima a través de atentados a la sana técnica informática, lo cual, generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, repontándose, muchas veces, un beneficio ilícito en el agente, sea o no sea caracter patrimonial, actúe con o sin ánimo de lucro.[27]

Rossini, compreende que o melhor conceito para “delito informático” é o usado pela Organização para Cooperação Econômica e Desenvolvimento da ONU: *o crime de informática é qualquer conduta ilegal não-ética, ou não-autorizada, que envolva processamento automático de dados e/ou transmissão de dado*s.[28]

Ferreira, define crime de informática como sendo *toda ação típica, antijurídica e culpável, cometida contra ou pela utilização de processamento automático de dados ou sua transmissão.*[29]

Por sua vez, Reginaldo César Pinheiro, entende crime informático como sendo: *toda conduta positiva ou negativa (ação ou omissão), praticada total ou parcialmente no ambiente informático e que venha causar algum prejuízo à vítima, seja ele patrimonial ou não.*[30]

No presente trabalho entendemos que delito informático pode ser entendido como uma conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, cometida 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.

---

[27] LÍBANO MANZUR, Claudio. "Chile: Los Delictos de Hacking en sus Diversas Manifestaciones", in Revista Electrónica de Derecho Informático, nº 21, abril de 2000. Disponível em: <http://publicaciones.derecho.org/redi>. Acesso em: 10 de abril de 2021.

[28] ROSSINI, Augusto Eduardo de Souza. Brevíssimas considerações sobre delitos informáticos. São Paulo: ESMP, jul. 2002. p. 140 (Caderno Jurídico, ano 02, n. 04).

[29]FERREIRA, Ivette Senise. A criminalidade informática. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto (coord.). Direito e internet: aspectos jurídicos relevantes.Bauru: Edipro. 2000, p. 210.

[30] PINHEIRO, Reginaldo César. Os crimes virtuais na esfera jurídica brasileira. São Paulo: IBCCrim, v. 101, abr. 2001, p. 18-19.

Frisa-se que o termo mais adequado seria delito informático, pois a expressão “delito” é genérica, na qual cabem tanto os “crimes” quanto às “contravenções penais”.

Portanto, o termo delito informático não se estende apenas às ações cometidas no âmbito da Internet, mas também a toda e qualquer ação relacionada com sistemas informáticos, seja de meio, ou de fim, sendo que essa denominação alcançaria os delitos em que o computador é mera ferramenta.

2.3 CLASSIFICAÇÃO DO DELITO PENAL INFORMÁTICO

Classificar os delitos praticados na internet é relevante para melhor compreensão e delimitação do assunto. Na doutrina contemporânea há diversas classificações sobre o tema. Abordaremos, adiante, algumas dessas classificações.

Ulrich Sieber dividiu os delitos informáticos em três grupos, considerando o bem jurídico afetado:

> a) crimes econômicos, que por seu turno se subdividem em a1) fraude por manipulação de dados em sistemas de processamento de dados; a2) espionagem de dados e pirataria de programas; a3) sabotagem; a4) furto de serviço ou furto de tempo; a5) acesso não autorizado a sistemas de processamento de dados; a6) uso do computador para crimes empresariais; b) ofensas contra direitos individuais, que se subdividem em: b1) uso incorreto de informação; b2) obtenção ilegal de dados e posterior arquivo das informações; b3) revelação ilegal e mau uso da informação; b4) dificuldade de se distinguir entre obtenção, arquivamento ou revelação de informações; e c)ofensas contra direitos supraindividuais, divididas em c1) ofensas contra interesses estaduais e políticos e c2) a extensão desta categoria para crimes contra a integridade humana.[31]

Por outro lado, Túlio Lima Vianna, acredita que os delitos informáticos se dividem em quatro grupos:

> 1) Delitos informáticos impróprios: são aqueles nos quais o computador é usado como instrumento para a execução do crime, mas não há ofensa ao

[31] The internacional handbook on computer crime. New York: John Wiley Sos, 1986, *apud* Sandra Gouvêa. O Direito na Era Digital: crimes praticados por meio da informática. Rio de Janeiro: Mauad, 1997. (Série Jurídica, v. 1), p. 62-65.

> bem jurídico inviolabilidade da informação automatizada (dados).
> 2) Delitos informáticos próprios: são aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados).
> 3) Delitos informáticos mistos: são crimes complexos em que, além da proteção da inviolabilidade dos dados, a norma visa a tutelar bem jurídico de natureza diversa.
> 4) Delito informático mediato ou indireto: é o delito-fim não informático que herdou esta característica do delito-meio
> informático realizado para possibilitar a sua consumação.[32]

Quanto à forma de cometimento, Ivette Senise Ferreira, divide os delitos informáticos em delitos próprios e impróprios[33]. Os crimes próprios, seriam aquelas condutas perpetradas contra um sistema informático, sejam quais forem as motivações do agente. E os crimes impróprios, seriam as condutas perpetradas contra outros bens jurídicos, por meio de um sistema informático, sendo que outros meios poderiam ter sido utilizados para a prática.

Na concepção de Spencer Toth Sydow (2021, p. 270), são três as formas de se perpetuar aquilo que se denomina delito informático:

> 1. Violando-se o bem jurídico informático em si, em seus elementos, fazendo uso de ferramentas comuns;
> 2. Utilizando-se do meio informático como instrumento para atacar bem jurídico diverso do informático; e
> 3. Violando-se o bem jurídico informático em si, em seus elementos, mas utilizando-se para isso exclusivamente de meios informáticos (portanto não ferramentas comuns).

Sendo assim, a classificação de delitos cibernéticos não apenas alcança as ações praticadas no ambiente virtual, mas toda conduta em que há relação com o sistema informático, seja como meio ou como fim. A denominação abrangerá até aquele delito em que o computador é mera ferramenta, de modo que delito digital é gênero.

Nessa conjuntura, como fator criminógeno, devemos observar que a rede mundial possibilita não só o cometimento de novos delitos, como intensifica alguns outros tradicionais (estelionato, por exemplo).

---

[32]VIANA, Tulio Lima. Do acesso não autorizado a sistemas computacionais: fundamentos de direito penal informático. Rio de Janeiro: Forense, 2003, p. 13-26.

[33] FERREIRA, Ivette Senise. A criminalidade informática. In: LUCCA, Newton de; SIMÃO FILHO, Adalberto (coord.). Direito e internet: aspectos jurídicos relevantes.Bauru: Edipro. 2000, p. 210.

2.4 SUJEITO ATIVO DO DELITO INFORMÁTICO

Os delitos informáticos não são cometidos apenas por indivíduos especialistas, longe disso, cada dia há maior acessibilidade a computadores e outros aparelhos conectados à internet, sendo este acesso associado ao crescimento da Internet.

Com a crescente evolução dos meios de comunicação, novos equipamentos, novas tecnologias, e maior acessibilidade, um usuário da rede com poucos conhecimentos da área pode se tornar um cibercriminoso.

O criminoso informático não é um hacker. Embora muitos de nós associamos o termo "hacker" aos cibercriminosos, essa não é a definição correta. Hacker é aquela pessoa que tem conhecimentos de informática, que pode programar, modificar *softwares*, invadir sistemas, encontrar brechas de segurança, por essa razão, há empresas que contratam hackers para melhorar seus sistemas de segurança[34].

O autor do delito informático pode ser qualquer usuário da rede, que tenha ou não conhecimentos aprofundados de informática. Claro que há delitos que necessitam de capacidade técnica elevada para serem cometidos, mas há também delitos que necessitam pouca ou nenhuma técnica especial para serem realizados.

O criminoso comum, que pratica crimes tradicionais, que poderiam ser realizados fora do ambiente virtual (estelionato, por exemplo), encontrou na internet um novo espaço para realizar suas condutas criminosas, devido às facilidades que o meio digital fornece, pela impunidade, pela crença que a internet é “terra de ninguém”. Ou até, pela falta de cuidado ou ingenuidade da vítima em confiar na segurança da internet.

Embora exista uma série de denominações para identificar os autores das condutas ilícitas cibernéticas, cabe apresentar a conceituação básica do sujeito

---

[34] BACH, Sirlei Lourdes. A contribuição do hacker para o desenvolvimento tecnológico da informática. 2001, p. 4 e 5.

hacker, classificatória e criada pelos próprios, quais sejam *White Hats, Grey Hats e Black Hats*[35].

Essas expressões significam, respectivamente, “chapéu branco”, “chapéu cinza” e “chapéu preto”, são expressões criadas na própria web, para diferenciar os hackers quanto à intenção lesiva (SYDOW, 2021, p. 326).

Os “chapéus brancos” são os hackers sem intenção de cometer crimes, que utilizam todo o seu conhecimento para melhorar programas e sistemas de segurança. (idem, p. 327).

Em sentido oposto, os “chapéus pretos” utilizam seus conhecimentos para violar bens jurídicos, ou seja, cometer delitos, também conhecidos como *crackers*, são os verdadeiros invasores de computadores e sistemas (idem, p. 326).

Para finalizar, os “chapéus cinzas”, são hackers que às vezes agem como o white hat, e outras vezes como um black hat, por exemplo, podem invadir um sistema sem causar danos, ver tudo que está nele, divulgar ou não a informação conseguida, mas não informa os administradores do sistema sobre a falha e nem toma atitude para corrigi-la (idem, p. 326).

2.5 SUJEITO PASSIVO DO CRIME INFORMÁTICO

O sujeito passivo do crime informático, é o ente que sofre uma ação ou omissão do sujeito ativo, e que tem seu bem jurídico violado. O sujeito passivo dos crimes de informática pode ser qualquer pessoa, física ou jurídica, de natureza pública ou privada.

No próximo capítulo falaremos especificamente sobre a vítima do delito informático.

---

[35] Saiba a diferença entre Hackers, Crackers, White Hat, Black Hat, Gray Hat, entre outros. E-GOV UFSC. Disponível em: https://egov.ufsc.br/portal/conteudo/saiba-diferen%C3%A7a-entre-hackers-crackers-white-hat-black-hat-gray-hat-entre-outros. Acesso em 30 de abril de 2021.

3. A VÍTIMA DO DELITO INFORMÁTICO SOB A ÓTICA DA VITIMOLOGIA

Dentro do campo da criminologia, há o ramo da vitimologia, que pesquisa a extensão, natureza e causas da vitimização criminal, bem como, estuda de forma ampla a vítima sob um aspecto amplo e integral: psicológico, social, econômico e jurídico.

A expressão "vitimologia" foi utilizada primeiro pelo psiquiatra americano Frederick Wertham, mas alcançou notoriedade com o trabalho de Hans von Hentig "The Criminal an his Victim", de 1948.

> Hentig propôs uma abordagem dinâmica, interacionista, desafiando a concepção de vítima como ator passivo. Salientou que poderia haver algumas características das vítimas que poderiam precipitar os fatos ou condutas delituosas. Sobretudo, realçou a necessidade de analisar as relações existentes entre vítima e agressor.[36]

Nesse sentido, segundo leciona José R. Agustina, Benjamin Mendelsohn, considerado juntamente com Hans von Hentig, um dos fundadores da vitimologia como um ramo independente de Criminologia, formulou com base em um estudo/questionário sobre suas vítimas-clientes, em seu trabalho como advogado, uma tipologia de vítimas que englobava diferentes graus de culpa (AGUSTINA, José R., 2014, p. 155). Em sua classificação, as vítimas foram classificadas da seguinte forma:

> Endicha clasificación, distinguía desde (1) víctimas completamente inocentes (por ej., un niño), hasta (2) víctimas a las que se atribuía la culpa en su totalidad (por ej., un ofensor que resultaba muerto por su víctima, actuando ésta en legítima defensa). Entre ambos extremos, Mendelsohn situaba tres tipos más de víctimas: (3) víctimas con una culpa menor, (4) víctimas tan culpables como el propio ofensor y (5) víctimas más culpables que su ofensor. (AGUSTINA, José R., 2014, p. 155).

A análise sobre as diferentes espécies de vítimas faz-se muito relevante para a prevenção do delito, pois oferece imensos subsídios sobre como, quem, quais circunstâncias de tempo e lugar, e por quais fatores os delitos são praticados. A vitimologia tem oferecido imensa contribuição para o entendimento do fenômeno

---

[36] Noções de Criminologia. Disponível em: <https://www.doraci.com.br/files/criminologia.pdf>. Acesso em: 04 de maio.

do crime, bem como, presta atenção às vítimas e aos danos causados, contribuindo para melhor enfrentamento da criminalidade.

3.1 CONSIDERAÇÕES VITIMOLÓGICAS APLICADAS AO CIBERESPAÇO

A partir dos anos 1990, a internet começou a se popularizar, hoje em dia é quase impossível imaginar um mundo sem internet, a internet não só invadiu as residências dos indivíduos, mas também seus trabalhos, as empresas, indústrias, todos viram impactos e mudanças.

Não trouxe apenas benefícios, mas também abriu espaço para condutas criminosas, novos delitos surgiram e delitos conhecidos passaram a ser praticados no ambiente virtual, com nova roupagem, nova dinâmica, novo *modus operandi.*

Um novo tipo de delinquente surgiu, com acesso a rede e a novas tecnologias que permitem praticar ações criminosas, dessa vez com a segurança do anonimato, e se beneficiando da falta de cuidado das vítimas.

Nessa série de mudanças que o mundo está vivendo, é imprescindível que um novo ramo criminológico surja, mesmo que a criminologia tradicional tenha fornecido um conjunto muito diverso de tipologias etimológicas ou classificações de tipos de vítimas em função da perspetiva adotada, a nova conjuntura e os delitos informáticos desafiam todas elas.

Spencer Sydow (2021, p.624), aponta que em 2007, Kuruppannan JAISHANKAR já desenvolvia o termo “cibercriminologia", *“para designar a ciência que estuda a causação dos crimes que ocorrem no cyberespaço e seus impactos no mundo físico”.*

Nesse sentido, a cibercriminlogia estuda o cibercriminoso, o comportamento do cibercriminoso, as cibervítimas, as ciberleis e a ciber investigação (SYDOW, 2021, p.625). Muitas são as esferas de pesquisa que esse novo ramo da criminologia terá de enfrentar.

> Nessa toada, é possível definir a cibercriminologia como a ciência multidisciplinar que reúne pesquisas de vários campos do saber como a criminologia clássica, a vitimologia, a sociologia da informação, a ciência da Internet, a ciência da computação, a estatística, a psicologia e a antropologia, entre outras (SYDOW, 2021, p.632).

Dentre as novas ideias que pretendem esclarecer o delito informático, a mais popular da cibercriminologia é chamada Teoria dos Espaços Transitórias ou Space Transition Theory. Segundo SYDOW, essa é a teoria mais adotada entre os estudiosos da cibercriminalidade:

> A teoria conjuga psicologia do delito, ambiência do delito (ecologia), hábitos informáticos, propensão delinquente e lógica internacional e conflitiva: A partir dela, sete premissas são apresentadas:
> (1) Pessoas reprimidas em suas vontades de cometer delitos no espaço físico tem propensão a cometer delitos no ciberespaço, especialmente porque não cometeriam os delitos na vida real pela posição que ocupam e pelo status que gozam;
> (2) A flexibilização da identidade, a anonimidade dissociativa e a ausência de um fator de constrição no ciberespaço estimulam a escolha por delinquir;
> (3) Há uma tendência a se importar ao mundo virtual o delito do mundo real pelos ganhos em velocidade, facilidade e abrangência;
> (4) A intermitência do ofensor no ciberespaço e a dinâmica da natureza espaço-temporal da virtualidade fazem com que haja sempre chance de escapar impune do delito;
> (5) Há uma dualidade agremiadora, associativa e recrutadora no ciberespaço: existe uma capacidade diferente do usual de reunião no ciberespaço, inclusive de agrupamento de totais estranhos, no intuito de cometerem um delito real. E há uma reunião de pessoas que se conhecem no mundo real que se reúnem para delinquir no ciberespaço;
> (6) Pessoas introspectivas encontram estímulo no ciberespaço para extravasarem seus sentimentos, e por isso, sentem-se à vontade para agir;
> (7) O conflito de normas internacionais ou a inexistência destas no ciberespaço facilita a ponderação pelo delito informático. (SYDOW, 2021, p. 640-641)

Sendo assim, a conduta do usuário da rede é o principal fator de risco para que o delito informático se desenvolva, e o então usuário da internet, passe a ser a vítima de um delito. Estudar o comportamento da vítima que a vítima apresenta nos crimes, é importantíssimo para desenvolver estratégias de prevenção afetivas.

Assim, o comportamento da vítima se torna, de alguma forma, uma co-causa de sua vitimização, vejamos:

> Por tanto, si se asume que la exposición voluntaria de la propia víctima ante potenciales ofensores permite y facilita su victimización, se puede concluir, aunque sea solo desde una perspectiva criminológica, que con su comportamiento deviene, de algún modo, co-causante de su propia victimización, en la medida en que estuvo en sus manos la posibilidad de evitar la interacción con su ofensor. (AGUSTINA, José R., 2014, p. 152)

Frisa-se que isso não significa culpar a vítima ou responsabilizá-la pelos danos que sofreu, ou diminuir e isentar o delinquente de sua responsabilidade

criminal, longe disso, mas há uma ligação entre a conduta do indivíduo que possivelmente terá seu bem violado e a conduta do vitimário.

José R. Agustina apresenta ambientes vitimológicos, e a partir deles, perfis vitimológicos, o autor elenca dois elementos importantes, o primeiro é, (a) Efeito de desinibição online: a primeira característica das vítimas no ciberespaço tem referência ao efeito desinibidor que o contexto digital exerce sobre elas. Nesse ambiente, os internautas se sentem menos restritos, mais soltos e se expressam de forma muito mais aberta do que em seus relacionamentos diretos (AGUSTINA, José R., 2014, p. 162). De acordo com José R. Agustina, o fenômeno já é tão generalizado que começou a ser chamado de “efeito desinibidor ”do ciberespaço no comportamento das pessoas. O autor, citando Suler, elenca as seguintes características de uma psicologia para o ciberespaço, listando os seguintes elementos:

> **(1) anonimidad disociativa:** la posibilidad de no revelar la propia identidad conlleva que, en virtud del anonimato, la persona pueda garantizar que no se vincule su actividad online con su persona en la vida “real”, disociando así ambas identidades; **(2) invisibilidad:** el hecho de que las personas puedan navegar a través de la red, entrando en páginas web o páginas de chat sin ser no solo identificados sino también sin que el resto de usuarios perciban su presencia, impulsa que se atrevan a visitar lugares que, de otro modo, nunca visitarían –sobre todo por vergüenza y por las consecuencias en su propia reputación–; **(3) asincronicidad:** en las comunicaciones en el ciberespacio muchas veces la interacción no se produce en tiempo real, al menos no necesariamente. Este hecho proporciona una mayor capacidad de pensar y editar la forma de presentarse, proporcionando mayor seguridad a los adolescentes46; y facilita que puedan darse situaciones en las que, tras una mayor reflexión o ante un momento de impulso, la persona llegue a escribir un mensaje muy personal, hostil o cargado de emociones y huir, fenómeno que podría describirse como un “emotional hit and run”; **(4) introyección solipsística:** fruto de la ausencia de datos fiables sobre la otra persona, puede producirse un efecto psicológico por el que el sujeto asigna características y rasgos a la persona o personas con las que interactúa en la red que, en realidad, son fruto de la propia imaginación. Las fantasías de la imaginación, pudiéndose dar también en la vida “real”, se ven potenciadas de forma considerablemente desinhibida en la red; **(5) imaginación disociativa:** de forma consciente o inconsciente, los internautas pueden llegar a percibir que los personajes imaginarios que ellos mismos “crearon” existen en un espacio diferente; que su yo-digital junto a esas otras personas online viven en otra dimensión, en sus sueños, separada de las exigencias y responsabilidades de su vida “real”. De este modo se produce una fragmentación o disociación entre el mundo de ficción online y los hechos de su vida real offline; **(6) minimización del status y autoridad:** en Internet todo el mundo parte, en cierto modo, de la misma posición, al estar todas las personas (aunque sean famosas o detenten alguna posición de autoridad), igualmente accesibles; y, por otro lado, el hecho de estar en la red conlleva que las personas con un cierto status o autoridad puedan perder los atributos visibles que en el mundo “real” le distancian del resto de mortales, con los efectos desinhibidores que ello conlleva. (AGUSTINA, José R., 2014, p. 163-164).

Os efeitos desinibidores do ciberespaço que José R. Agustina descreve, claramente, são fatores que aumentam a probabilidade de os usuários incorrerem em comportamentos de risco e acabam sendo cibervitimizados. A desinibição, portanto, leva a vítima a ultrapassar o limite de risco.

O segundo elemento é: (b) Vítimas ingênuas e irreflexivas, junto com o efeito desinibidor estrutural ou situacional que geralmente influencia o comportamento online, vale a pena ter em mente o impacto especial da cultura digital nas gerações que cresceram e desenvolveram desde a primeira infância em um ambiente digitalizado. (idem, p. 165). Nesse sentido:

> En todo caso, el efecto desinhibidor en la persona (derivado de un entorno digitalizado) genera una aceleración de la conducta en una dinámica en el uso de las TIC que reviste con frecuencia tintes compulsivos, y se traslada a la esfera decisional del sujeto en términos de una mayor confianza o relajación en sus interacciones (ingenuidad) y en una ausencia de reflexividad en sus procesos de toma de decisiones (irreflexividad). Tales rasgos conductuales nos acercarían así a afirmar que el ciberespacio, de hecho, puede poseer un efecto determinante en los niveles de autocontrol del individuo. (AGUSTINA, José R., 2014, p. 165-166)

3.2 PREVENÇÃO DOS DELITOS INFORMÁTICOS

O ciberespaço tornou-se um ambiente propício para a prática de crimes, a vítima do delito informático confia na internet e acaba vulnerabilizada.

Na circunstância de crime tradicional, o indivíduo busca se proteger do delito, por exemplo, prefere carregar consigo cartões de crédito ao invés de dinheiro em espécie, evita transitar por ruas pouco iluminadas a noite e por lugares desconhecidos, não deixa os filhos irem para a escola sozinhos, enfim, o indivíduo tenta se proteger.

O cibercriminoso, assim como o criminoso tradicional procuraria a vítima que ele acredita ser mais frágil, para que a ação criminosa seja bem sucedida, age do mesmo jeito, procurando falhas na rede e indivíduos negligentes. Quanto mais possibilidades de cometer delitos, mais delitos aconteceram.

Diferentemente do delito tradicional, o delito informático invade sua esfera de vida privada, intimidade, residência, e os prejuízos podem ser imensuráveis.

Imagine o indivíduo que tinha uma foto íntima exposta por um ex companheiro, há 20 anos, o dano era muito mais restrito e controlável, agora imagine essa exposição em 2021, com redes sociais que alcançam milhões de pessoas, o dano é muito mais severo.

O usuário deve entender como é importante que ele haja de forma cautelosa quando navega na internet. A educação informática é essencial para a proteção do indivíduo e a prevenção dos crimes.

O delito informático não é de responsabilidade só do indivíduo, mas, obviamente, dos governos e autoridades. A população carece de educação informática que necessita ser ensinada nas escolas, educação nunca é demais.

Há alguns anos, uma ex-presidente do país foi vítima de espionagem, por outro Estado, e pasmem, não houve aumento dos investimentos em cibersegurança.

A resposta estatal para a prevenção desses delitos é lenta. O Brasil, hoje, não possui legislação específica sobre o tema, o Marco Civil da Internet, a Lei Carolina Dieckmann e a Lei Geral de Proteção de Dados não são suficientes e adequadas a essa nova realidade.

Portanto, a postura do usuário no ciberespaço é muito significativa para sua própria proteção. É importante adotar alguns cuidados, mantenha os programas antivírus atualizados, troque as senhas de acesso a contas online com frequência, não utilize a mesma senha para diferentes serviços, não empreste senhas ou chaves de acesso, utilize o cartão de crédito em compras online apenas em sites confiáveis, não acesse sites suspeitos, utilize redes Wi-Fi confiáveis, desconfie de mensagens de desconhecidos e analise os links e remetentes dos e-mails antes de clicar, entre outras.

4. CONSIDERAÇÕES FINAIS

Compreendendo que o tema abordado é de extrema relevância para o direito, vez que a internet e a tecnologia estão inseridas na vida cotidiana das pessoas e que é crescente a criminalidade informática, cumpre aos operadores do direito buscar formas de prevenção dos cibercrimes.

Como discutido anteriormente, para a prevenção desse tipo delituoso, é de suma importância estudar os aspectos vitimológicos que existem por trás desses delitos, traçar as características da vítima, e como o ambiente que ela está inserida influência nos riscos que ela está sujeita.

Após estudar e assimilar através de leituras críticas e analíticas, entendo que a temática precisa ser evidenciada e tratada de forma emergente, considerando que o ambiente digital é nosso futuro, e como tal, deve se tornar um lugar mais seguro e de riscos controlados.

REFERÊNCIAS BIBLIOGRÁFICAS

AGUSTINA, José R. **Cibercriminalidad y perspectiva victimológica: un enfoque general explicativo de la cibervictimización.** Cuadernos de política criminal. Número 114, III, Época II. 2014, p. 143-178.

BACH, Sirlei Lourdes. **A contribuição do hacker para o desenvolvimento tecnológico da informática**. 2001, p. 4 e 5.

Backbone da RNP em Santa Catarina no ano 1996 (Arquivo Histórico). Memória da internet acadêmica em Santa Catarina. Publicado em: agosto de 2017. Disponível em: <https://memoria.pop-sc.rnp.br/backbone_rnp_1996/>.Acesso em: 19 de março de 2021.

BARBAI. M.A. **A criminalidade no espaço digital; a formulação do sentido**. In. DIAS, Cristiane. Formas de mobilidade no espaço e-urbano: sentido e materialidade digital [online]. (Serie e-urbano, v.2). 2013, p. 48, Disponível em: <https://www.labeurb.unicamp.br/livroEurbano/>. Acesso em: 10 de abril de 2021.

BRASIL. **Código Penal**, Decreto-lei n°2.848, de 07 de dezembro de 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 06 de abril de 2021.

BRASIL. **Constituição da República Federativa do Brasil de 1998.** Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 07 de abril de 2021.

BRASIL. **Lei Carolina Dieckmann**, Lei n° 12.737/2012, de 30 de novembro de 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 02 de abril de 2021.

BRASIL. **Marco Civil da Internet,** Lei n° 12.965/14, de 23 de abril de 2019. Disponível em:

<http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 27 de março de 2021.

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, p. 11.

CAPEZ, Fernando. **Curso de Direito Penal:** *parte geral***.** 1. São Paulo: Saraiva. 15° ed. 2011, p. 19.

CLEMENTE, Rafael. **A World Wide Web completa 25 anos. Em 12 de março de 1989 o britânico Tim Berners-Lee descreveu o protocolo de transferências de hipertextos.** El País. Disponível em: <https://brasil.elpais.com/brasil/2014/03/11/tecnologia/1394554623_973239.html#:~:text=Em%2012%20de%20mar%C3%A7o%20de,protocolo%20de%20transfer%C3%AAncias%20de%20hipertextos&text=Em%2012%20de%20mar%C3%A7o%20de%201989%2C%20o%20pesquisador%20brit%C3%A2nico%20Tim,seria%20a%20World%20Wide%20Web>. Acesso em: 16 de março de 2021.

Convenção de Budapeste sobre Crimes Cibernéticos. Disponível em: <http://www.mpf.mp.br/atuacao-tematica/sci/normas-e legislacao/legislacao/legislacoes-pertinentes-do brasil/docs_legislacao/convencao_cibercrime.pdf>. Acesso em: 25 de março de 2021.

Denúncias de crimes cometidos pela internet mais que dobram em 2020. G1 Globo. Publicado em: 09 de fevereiro de 2021. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2021/02/09/numero-de-denuncias-de-crimes-cometidos-pela-internet-mais-que-dobra-em-2020.ghtml>. Acesso em: 15 de março de 2021.

FERNANDEZ, Marcial Porto. **Rede de Computadores**. Ceará. Ed. UECE. 2015. Disponível em: <http://www.uece.br/computacaoead/index.php/downloads/doc_download/2100-redescomputadores>. Acesso em: 16 de março de 2021.

FERREIRA, Ivette Senise. **A criminalidade informática.** In: LUCCA, Newton de; SIMÃO FILHO, Adalberto (coord.). Direito e internet: aspectos jurídicos relevantes.Bauru: Edipro. 2000, p. 210.

História da internet no Brasil. Disponível em: <https://homepages.dcc.ufmg.br/~mlbc/cursos/internet/historia/Brasil.html>. Acesso em: 17 de março de 2021.

JESUS, Damásio. **Direito Penal: parte geral**. São Paulo: Saraiva. 32° ed. 2011, p. 45.

LÍBANO MANZUR, Claudio. **"Chile: Los Delictos de Hacking en sus Diversas Manifestaciones"**. In Revista Electrónica de Derecho Informático, nº 21, abril de 2000. Disponível em: <http://publicaciones.derecho.org/redi>. Acesso em: 10 de abril de 2021.

MONTEIRO, Luís. **A INTERNET COMO MEIO DE COMUNICAÇÃO: POSSIBILIDADES E LIMITAÇÕES.** 2001, p.28.

Nossa história. Rede Nacional de Ensino e Pesquisa. Disponível em: <https://www.rnp.br/sobre/nossa-história>. Acesso em: 17 de março de 2021.

Nota conjunta do Ministério da Ciência e Tecnologia e Ministério das Comunicações (maio de 1995). Comitê Gestor da Internet no Brasil (CGI.br). Disponível em: <https://www.cgi.br/legislacao/notas/nota-conjunta-mct-mc-maio-1995#:~:text=1.1%20O%20Governo%20considera%20de,%2C%20preferencialmente%2C%20pela%20iniciativa%20privada>. Acesso em: 19 de março de 2021.

Noções de Criminologia. Disponível em: <https://www.doraci.com.br/files/criminologia.pdf>. Acesso em: 04 de maio.

Pacto Internacional de Direitos Civis e Políticos. Decreto n° 592, de 06 de julho de 1992. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm>. Acesso em: 25 de março de 2021.

PINHEIRO, Reginaldo César. **Os crimes virtuais na esfera jurídica brasileira.** São Paulo: IBCCrim. v. 101. 2001, p. 18-19.

Relatório da ONU declara internet como um direito humano. Tecnologia Terra. Publicado em: 6 de junho de 2011. Disponível em: <http://tecnologia.terra.com.br/internet/relatorio-da-onu-declara-internet-como-um-direito-humano,8ea9dceae77ea310VgnCLD200000bbcceb0aRCRD.html>. Acesso em: 15 de março de 2021.

ROSSINI, Augusto Eduardo de Souza. **Brevíssimas considerações sobre delitos informáticos**. São Paulo: ESMP. (Caderno Jurídico, ano 02, n. 04). jul. 2002, p. 140

Saiba a diferença entre Hackers, Crackers, White Hat, Black Hat, Gray Hat, entre outros. E-GOV UFSC. Publicado em: 18 de junho de 2016. Disponível em: <https://egov.ufsc.br/portal/conteudo/saiba-diferen%C3%A7a-entre-hackers -crackers-white-hat-black-hat-gray-hat-entre-outros>. Acesso em 30 de abril de 2021.

SYDOW, Spencer Toth. Curso **de Direito Penal Informático: partes geral e especial.** Salvador: Juspodivm. 2° ed. 2021.

The internacional handbook on computer crime. New York: John Wiley Sos, 1986, *apud* Sandra Gouvêa. O Direito na Era Digital: crimes praticados por meio da informática. Rio de Janeiro: Mauad, 1997. (Série Jurídica, v. 1), p. 62-65.

TIC Domicílios 2019. Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação. Publicado em: 26 de maio de 2020. Disponível em:

<https://cetic.br/media/analises/tic_domicilios_2019_coletiva_imprensa.pdf>. Acesso em: 15 de março de 2021.

VIANA, Tulio Lima. **Do acesso não autorizado a sistemas computacionais: fundamentos de direito penal informático**. Rio de Janeiro: Forense. 2003, p. 13-26.

TERMO DE AUTENTICIDADE DO TRABALHO DE CONCLUSÃO DE CURSO

Eu, Alessandra Navarro Hamid, discente regularmente matriculada na disciplina TCC II, da 10ª etapa do curso de Direito, matrícula nº 41680561, período noturno, turma U, tendo realizado o TCC com o título: Cibercriminalidade: aspectos vitimológicos sobre os delitos informáticos, sob a orientação da Professora Dra. Thamara Duarte Cunha Medeiros declaro para os devidos fins que tenho pleno conhecimento das regras metodológicas para confecção do Trabalho de Conclusão de Curso (TCC), informando que o realizei sem plágio de obras literárias ou a utilização de qualquer meio irregular.

Declaro ainda que, estou ciente que caso sejam detectadas irregularidades referentes às citações das fontes e/ou desrespeito às normas técnicas próprias relativas aos direitos autorais de obras utilizadas na confecção do trabalho, serão aplicáveis as sanções legais de natureza civil, penal e administrativa, além da reprovação automática, impedindo a conclusão do curso.

São Paulo, 21 de maio de 2021.

Alessandra Navarro Hamid

TERMO DE AUTORIZAÇÃO PARA PUBLICAÇÃO DO TRABALHO DE CONCLUSÃO DE CURSO

Material Bibliográfico: (X) Artigo Científico ( )Monografia
Graduação em Direito
Título do Trabalho: Cibercriminalidade: aspectos vitimológicos sobre os delitos informáticos
Nome do Autor(a): Alessandra Navarro Hamid
E-mail: alessandra.hamid@hotmail.com
Este e-mail pode ser divulgado (X) SIM ( ) NÃO
Orientadora: Prof° Dra. Thamara Duarte Cunha Medeiros

Na qualidade de titular dos direitos autorais da publicação supracitada, de acordo com a Lei nº 9.610/98, (X) AUTORIZO ( ) NÃO AUTORIZO a Universidade Presbiteriana Mackenzie – UPM, a disponibilizar gratuitamente, sem ressarcimento dos direitos autorais, o documento, em meio eletrônico, no *site* da base de dados Adelpha, para fins de leitura pela internet, a título de divulgação da produção científica gerada pela Universidade, a partir desta data. Igualmente, declaro que a versão do Trabalho de Conclusão de Curso entregue em meio eletrônico corresponde fielmente e na integra à versão similar depositada de forma impressa em papel para a defesa ou apresentação.

Motivos no Caso de Não Autorização
( )Exigência de periódico de não divulgação até a publicação (exige justificativa, informe e nome do periódico)
( )Outros (justificar): _____

_____

São Paulo, 21 de maio de 2021.

Alessandra Navarro Hamid