UNIVERSIDADE DO VALE DO ITAJAÍ – UNIVALI
VICE-REITORIA DE PESQUISA, PÓS-GRADUAÇÃO E EXTENSÃO
PROGRAMA DE PÓS-GRADUAÇÃO STRICTO SENSU EM CIÊNCIA JURÍDICA – PPCJ
CURSO DE MESTRADO EM CIÊNCIA JURÍDICA – CMCJ
ÁREA DE CONCENTRAÇÃO: FUNDAMENTOS DO DIREITO POSITIVO
LINHA DE PESQUISA: DIREITO, JURISDIÇÃO E INTELIGÊNCIA ARTIFICIAL

PROJETO DE PESQUISA INTERNACIONAL CONJUNTO PPCJ/UNIVALI E A *FACOLTÁ DE GIURISPRUDENZA* DA UNIVERSIDADE DE PERUGIA – ITÁLIA

PROJETO DE PESQUISA: DIREITO E INTELIGÊNCIA ARTIFICIAL

Crimes Cibernéticos – Seus desafios para a Polícia Judiciária Brasileira e as Melhores Técnicas Investigativas e Procedimentos a serem adotados para enfrentamento dessa modalidade delitiva

Rodrigo Souza Barreto

Itajaí-SC
2023

UNIVERSIDADE DO VALE DO ITAJAÍ – UNIVALI
VICE-REITORIA DE PESQUISA, PÓS-GRADUAÇÃO E EXTENSÃO
PROGRAMA DE PÓS-GRADUAÇÃO STRICTO SENSU EM CIÊNCIA JURÍDICA – PPCJ
CURSO DE MESTRADO EM CIÊNCIA JURÍDICA – CMCJ
ÁREA DE CONCENTRAÇÃO: FUNDAMENTOS DO DIREITO POSITIVO
LINHA DE PESQUISA: DIREITO, JURISDIÇÃO E INTELIGÊNCIA ARTIFICIAL

PROJETO DE PESQUISA INTERNACIONAL CONJUNTO PPCJ/UNIVALI E A *FACOLTÁ DE GIURISPRUDENZA* DA UNIVERSIDADE DE PERUGIA – ITÁLIA

PROJETO DE PESQUISA: DIREITO E INTELIGÊNCIA ARTIFICIAL

Crimes Cibernéticos – Seus desafios para a Polícia Judiciária Brasileira e as Melhores Técnicas Investigativas e Procedimentos a serem adotados para enfrentamento dessa modalidade delitiva

Rodrigo Souza Barreto

Dissertação submetida ao Curso de Mestrado em Ciência Jurídica da Universidade do Vale do Itajaí – UNIVALI, como requisito parcial à obtenção do título de Mestre em Ciência Jurídica. Em dupla titulação com a Università Degli Studi di Perugia - UNIPG

Orientador: Professor Doutor Alexandre Morais da Rosa

Itajaí-SC
2023

AGRADECIMENTOS

Primeiramente, à Deus por proporcionar e mostrar que tudo é possível.

Aos professores do Mestrado que tanto contribuíram para meu conhecimento e ajudaram a expandir minha mente para outras áreas do direito.

Á Profa. Doutora Maria Claudia Antunes de Souza por todo o incentivo, paciência e acreditar sempre em todos, sendo uma fonte de inspiração.

Aos meus amigos que contribuíram de alguma forma para a consecução da tese final, nas sugestões, cedendo livros e incentivando a seguir em frente.

Aos meus pais por todo suporte e por sempre acreditarem em mim.

Aos dois grandes amores da minha vida Priscila e minha filha Luíza, pela paciência, incentivo e auxílio. Sempre mostrando que era possível e nunca me deixando desistir.

DEDICATÓRIA

Dedico esse trabalho aos meus pais, a minha esposa Priscila e a minha filha Luíza.

TERMO DE ISENÇÃO DE RESPONSABILIDADE

Declaro, para todos os fins de direito, que assumo total responsabilidade pelo aporte ideológico conferido ao presente trabalho, isentando a Universidade do Vale do Itajaí, a Coordenação do Curso de Mestrado em Ciência Jurídica, a Banca Examinadora e o Orientador de toda e qualquer responsabilidade acerca do mesmo.

Itajaí-SC, fevereiro de 2023.

Rodrigo Souza Barreto
Mestrando

P Á G I N A D E A P R O V A Ç Ã O

MESTRADO

Conforme Ata da Banca de Defesa de Mestrado, arquivada na Secretaria do Programa de Pós-Graduação *Stricto Sensu* em Ciência Jurídica PPCJ/UNIVALI, em 04/04/2023, às doze horas (Horário de Brasília), dezessete horas (Horário em Perugia), o mestrando Rodrigo Souza Barreto fez a apresentação e defesa da Dissertação, sob o título "Crimes Cibernéticos – Seus desafios para a Polícia Judiciária Brasileira e as Melhores Técnicas Investigativas e Procedimentos a serem adotados para enfrentamento dessa modalidade delitiva".

A Banca Examinadora foi composta pelos seguintes professores: Doutor Alexandre Morais da Rosa (UNIVALI), como presidente e orientador, Doutor Francesco Paolo Micozzi (UNIPG), como coorientador, Doutora Dirajaia Esse Pruner (UNIVALI), como membro e Doutora Jaqueline Moretti Quintero (UNIVALI), como membro suplente. Conforme consta em ata, após a avaliação dos membros da Banca, a Dissertação foi aprovada.

Por ser verdade, firmo a presente.

Itajaí (SC), 04 de abril de 2023.

PROF. DR. PAULO MÁRCIO DA CRUZ

Coordenador/PPCJ/UNIVALI

SUMÁRIO

RESUMO.....09

RIASSUNTO. 10

INTRODUÇÃO 11

CAPÍTULO 1

1. O Princípio da Dignidade da Pessoa Humana como base de tutela dos dispositivos que elencam os crimes cibernéticos 16

1.1 Definição e Previsão Legal dentro do Ordenamento Jurídico Brasileiro 16

1.2 A Dignidade da Pessoa Humana como Direito Fundamental 20

1.3 A ofensa aos diversos bens jurídicos no cometimento dos crimes de internet em paralelo com o desrespeito à dignidade da pessoa humana 22

1.4 O princípio da dignidade da pessoa humana como escopo máximo de proteção da legislação que estabelece os crimes digitais 24

CAPÍTULO 2

2. Dos Crimes Cibernéticos 26

2.1 O início de uma nova era – A Era Digital 26

2.2 Dos crimes cibernéticos 29

2.2.1 Os crimes cibernéticos propriamente ditos 31

2.2.2 Delitos virtuais abertos..... 33

2.2.3 Delitos exclusivamente virtuais 34

2.2.4 Dos crimes de internet na sua forma imprópria 35

2.3 Os tipos de cybercrimes impróprios de maior incidência no cenário brasileiro 36

2.3.1 Invasão de Dispositivo Informático 37

2.3.2 Dano Informático 39

2.3.3 Interceptação clandestina de dados informáticos e telemáticos 42

2.3.4 Instalação de vírus e malwares com o cunho de se obter vantagem ilícita 43

2.4 Os tipos de cybercrimes impróprios de maior incidência no cenário brasileiro 45

2.4.1 Crimes contra a Vida 46

2.4.1.1 Auxílio, Induzimento e Instigação ao Suicídio 46

2.4.2 Crimes contra a Honra.....50

2.4.3 Ameaça 53

2.4.4 Crimes Contra o Patrimônio..... 55

2.4.4.1 Furto Eletrônico 55

2.4.4.2 Extorsão 58
2.4.4.3 Estelionato Eletrônico 60
2.4.5 Incitação e Apologia ao Crime 64
2.4.6 Falsa Identidade 66
2.4.7 Crimes contra a Dignidade Sexual 69
2.4.7.1 Estupro Virtual 69
2.5 Do Arcabouço legislativo no ordenamento jurídico brasileiro como base para proteção de direitos e o combate aos delitos digitais 71
2.5.1 Emenda Constitucional nº 115/2022 72
2.5.2 Lei Geral de Proteção de Dados 74
2.5.3 Lei 12.965/2014 (Marco Civil da Internet) 76
2.5.4 Lei 12.737/12 (Carolina Dieckmann) e o Decreto Lei 2848 de 1940 (Código Penal Brasileiro) 79
2.6 Da Transnacionalidade dos crimes cibernéticos 80
2.7 Crimes Cibernéticos de maior incidência durante a Pandemia provocada pelo vírus da Covid-19 85
2.8 O uso de dados telemáticos na investigação dos crimes virtuais e a necessidade de relativização dos princípios da privacidade e intimidade 92

CAPÍTULO 3

3. Os desafios na investigação dos crimes cibernéticos e o uso das melhores técnicas investigativas e procedimentais para identificação de autoria e formação de provas para o combate dessa modalidade delitiva 103
3.1 Dos desafios enfrentados pela polícia judiciária frente aos delitos virtuais 103
3.2 Os delitos cibernéticos mais comuns no momento atual e as técnicas utilizadas para identificação da autoria e materialidade 107
3.2.1 Sextorsão e as técnicas adotadas para investigação criminal 108
3.2.2 Estelionato Eletrônico 113
3.2.3 Crimes contra honra e o uso dos falsos perfis 117
3.2.4 Revenge Porn 119

CONCLUSÃO 124

REFERÊNCIA DAS FONTES CITADAS 127

RESUMO

A presente dissertação está inserida na linha de pesquisa “Direito, Inteligência Artificial e Jurisdição” e no projeto de pesquisa “Direito e Inteligência Artificial”, na Área de Concentração dos Fundamentos do Direito Positivo, do Curso de Mestrado em Ciência Jurídica, vinculado ao Programa de Pós-Graduação Stricto Sensu em Ciência Jurídica, da Universidade do Vale do Itajaí (UNIVALI), em regime de dupla titulação com Master di I Livello en Data Protection, Cybersecurity and Digital Forensics - Universidade de Perugia (UNIPG) – Itália, e Mestrado Interinstitucional com a Centro Universitário do Amazonas (CIESA). Como objetivo geral busca-se analisar a forma que a polícia judiciária brasileira aborda os crimes cibernéticos e quais são as melhores técnicas e procedimentos adotados para enfrentar esta modalidade criminosa. O presente trabalho procura responder o seguinte problema: Com a forte crescente do cometimento dos crimes virtuais, principalmente após o isolamento social consequente da pandemia do vírus da Covid 19, a polícia judiciária brasileira encontra-se preparada para lidar com a nova espécie delitiva, quais técnicas e procedimentos poderiam ser adotados para melhor proteger os bens jurídicos das vítimas? Foi utilizada como metodologia a pesquisa qualitativa, pesquisa bibliográfica e documental com a utilização de artigos, teses, dissertações e legislações nacionais e estrangeiras que tratam sobre o tema abordado. Para tanto, inicialmente serão feitas breves considerações acerca da tutela da dignidade da pessoa humana como cerne dos direitos protegidos no escopo da legislação que aborda os crimes virtuais. Em seguida, haverá uma melhor explanação sobre os crimes cibernéticos, seu conceito e classificação, além da previsão dentro do ordenamento jurídico pátrio, suas características e efeitos advindos do crescente aumento do acesso de pessoas à rede mundial de computadores. Após isso, serão apontados os principais desafios enfrentados pela polícia judiciária, apresentados os crimes de internet mais corriqueiros no país e abordado as melhores técnicas investigativas para combater esses delitos. Conclui-se que diante das dificuldades, necessita-se de um manual de técnicas e procedimentos investigativos dos principais crimes virtuais, como forma de padronizar a capacitação e orientação dos policiais no combate a uma categoria delitiva que vem atingindo uma imensa quantidade de vítimas em todo o país, uma vez que a atual forma de abordagem demonstra ser obsoleta e, dificilmente, contribuirá para identificar a autoria e existência desses novos delitos.

PALAVRAS CHAVE: CRIME CIBERNÉTICO, POLÍCIA JUDICIÁRIA, DESAFIOS, INVESTIGAÇÃO.

RIASSUNTO

Questa tesi fa parte della linea di ricerca "Diritto, Intelligenza Artificiale e Giurisdizione" e del progetto di ricerca "Diritto e Intelligenza Artificiale", nell'area di concentrazione dei Fondamenti del Diritto Positivo, del Corso di Laurea Magistrale in Scienze Giuridiche, collegato al Programma Stricto Sensu Postgraduate in Scienze Giuridiche dell'Università di Vale do Itajaí (UNIVALI), in regime di doppio titolo con un Master in Data Protection, Cybersecurity and Digital Forensics - Università di Perugia (UNIPG) - Italia, e un Master interistituzionale con il Centro Universitario di Amazonas (CIESA). L'obiettivo generale è analizzare come la polizia giudiziaria brasiliana si approccia alla criminalità informatica e quali sono le migliori tecniche e procedure adottate per affrontare questo tipo di crimine. Questo lavoro cerca di rispondere al seguente problema: con il forte aumento della criminalità informatica, soprattutto dopo l'isolamento sociale derivante dalla pandemia del virus Covid-19, la polizia giudiziaria brasiliana è preparata ad affrontare questo nuovo tipo di crimine e quali tecniche e procedure potrebbero essere adottate per proteggere meglio i beni legali delle vittime? La metodologia utilizzata è stata quella della ricerca qualitativa, bibliografica e documentale, con l'ausilio di articoli, tesi, dissertazioni e legislazioni nazionali e straniere sull'argomento. A tal fine, inizieremo considerando brevemente la protezione della dignità della persona umana come il nucleo dei diritti tutelati nell'ambito della legislazione che si occupa dei crimini virtuali. Successivamente, si illustrerà meglio la criminalità informatica, il suo concetto e la sua classificazione, nonché la sua previsione all'interno dell'ordinamento giuridico nazionale, le sue caratteristiche e gli effetti derivanti dal crescente accesso delle persone alla rete di ampiezza mondiale. In seguito, saranno evidenziate le principali sfide che la polizia giudiziaria deve affrontare, saranno presentati i reati via Internet più comuni nel Paese e saranno discusse le migliori tecniche investigative per combattere questi reati. La conclusione è che, viste le difficoltà, è necessario un manuale di tecniche e procedure investigative per i principali crimini virtuali, in modo da uniformare la formazione e l'orientamento degli agenti di polizia nella lotta a una categoria di reati che sta colpendo un numero enorme di vittime in tutto il Paese, poiché l'approccio attuale si sta rivelando obsoleto e difficilmente può aiutare a identificare la paternità e l'esistenza di questi nuovi reati.

PAROLE CHIAVE: CRIMINALITÀ INFORMATICA, POLIZIA GIUDIZIARIA, SFIDE, INDAGINI.

INTRODUÇÃO

No presente momento, é raro conhecer alguém que não possua um smartphone e não faça dele um meio para navegar na internet. A era digital transformou o universo de todos e tornou uma imensidão de atividades mais práticas e acessíveis ao coletivo. A revolução tecnológica permitiu o surgimento de novos dispositivos que aceleraram a inclusão digital da população global, ao mesmo tempo eliminou fronteiras, aproximou pessoas e deu cabo ao aparecimento de novas profissões derivadas dessa área.

A amplitude da conexão das pessoas à internet contribui para desburocratizar serviços, facilitar as compras e, principalmente, a comunicação, aproximando muitas regiões do globo do seu isolamento geográfico.

Na proporção que cresceu o acesso à rede mundial de computadores, com o avanço da tecnologia 4.0 e comercialização em massa dos telefones inteligentes, surgiu um novo nicho de delitos capazes de atingir os indivíduos dentro da sua atividade rotineira.

Com a pandemia causada pelo vírus do Covid 19, os governos implantaram o necessário isolamento social como forma de combater a propagação em massa da doença, a destacada medida tornou-se fator preponderante para a conexão recorde em todo o mundo à rede mundial de computadores. No entanto, o distanciamento das ruas e dos serviços convencionais contribuiu para quase uma totalidade dos serviços migrarem para o âmbito virtual, fato que colaborou de forma significativa para a substituição da modalidade criminosa.

O objetivo institucional da presente Dissertação é a obtenção do título de Mestre em Ciência Jurídica pelo Curso de Mestrado em Ciência Jurídica da Univali. Vale ressaltar que se trata de um mestrado interinstitucional com dupla titulação com a Università Degli Studi Di Perugia – UNIPG.

A linha de pesquisa do presente trabalho se enquadra em direito, inteligência artificial e jurisdição. A área de concentração do curso são os fundamentos do direito positivo.

O projeto de pesquisa se concentrou nas àreas de inteligência artifical e direito. No entanto é possível constatar que buscou apontar as dificuldades enfrentadas pela polícia judiciária quando submetida à necessidade de investigação dos crimes virtuais, bem como quais desafios enfrentados e a necessidade de se estabelecer uma padronização da abordagem a este catálogo de delito e quais técnicas investigativas poderiam ser adotadas.

A importância do tema para a academia e a sociedade, se mostra devido à grande crescente dos delitos cometidos via internet, restou demonstrado a necessidade de detalhar o *modus operandi* dos autores como forma de dar melhor embasamento e subsidio para os atores da polícia judiciária no desempenho da persecução penal.

A substituição do tipo de crime deu margem para que alguns já existentes cambiassem para sua forma virtual, como exemplo do estelionato, furto eletrônico, do estupro virtual e a numerosa quantidade de delitos contra a honra cometidos através da internet. Por outro lado, crimes digitais propriamente ditos como invasão de dispositivo eletrônico cresceu de forma assustadora e incontrolável.

De fato, as delegacias de polícia em todo o Brasil não estavam preparadas para absorver, não só na quantidade, como nessa espécie delitiva. De certa forma nitidamente ficou exposto a falta de preparo técnico e o desconhecimento quanto a matéria para que se pudesse conferir o atendimento especializado aos diretamente afetados.

Mesmo com o surgimento de delegacias de combate aos crimes cibernéticos, restou impossível absorver mais que 10% do delito específico. Dessa forma, nasceu um grande desafio para os agentes de investigação no âmbito das polícias judiciárias.

É perceptível que a numerosidade de bens jurídicos atingidos pelos crimes de internet ofendem não só direitos primordiais ao ser humano como atinge no seu âmago a dignidade da pessoa humana, princípio constitucional base que é considerado fundamento e objetivo da Republica Federativa do Brasil.

Por isso, todo e qualquer dispositivo que estabelece algum crime digital contra a pessoa, protege algum bem jurídico, como vida, honra, dignidade sexual e patrimônio, assim como tutela a dignidade da pessoa humana.

Portanto, os aplicadores da lei, incluam-se neste rol, os agentes de polícia que labutam na esfera investigativa, protegem toda e qualquer pessoa da infringência a um direito positivado, mas que conta como escopo máximo a proteção e garantia da dignidade do ser humano.

Os delitos ditos cibernéticos têm como classificação principal ser próprio ou impróprio. O modelo próprio é inserido dia após dia no ordenamento jurídico brasileiro, a partir do momento que novas condutas impuníveis tornam-se corriqueiras e o legislador sente a necessidade de abordá-la e exprimi-la no corpo de uma lei. Por outra face, aqueles mencionados como impróprios são antigos crimes que os infratores utilizam a web como instrumento de cometimento.

A própria Constituição Federal de 1988, entende que é necessário reconhecer os dados pessoais digitais como uma espécie de direito merecedora de escopo e os posiciona como direito fundamental à pessoa. Na mesma linha, leis como o Marco Civil da Internet, que passa a criar regramento, estabelecendo direitos e deveres para aqueles que militam no ambiente virtual, exercem uma função demasiadamente importante quanto a lei apelidada como Carolina Dieckmann, que cria novos crimes digitais e os incluem dentro do Código Penal Brasileiro.

Entretanto, de certa forma, mesmo com o surgimento de um leque legislativo de regulação e proteção dos direitos das pessoas usuárias do ciberespaço, é perceptível como a polícia investigativa se encontra numa posição distante de colocar tais dispositivos normativos em prática.

Alguns fatores como: ausência de expertise, falta de estrutura, carência de corpo técnico especializado e inexistência de procedimento padrão de técnicas, que possam contribuir para uma melhor definição da autoria e identificação de materialidade dos crimes, aparecem como uma importante barreira a ser transposta pela Polícia Judiciária dos Estados.

O constante surgimento de delitos digitais denota a incapacidade do Poder Público de conseguir frear essa grande escalada de novos delitos, deixando clarividente a ausência de atualização do seu corpo técnico para que consiga enfrentar infrações que culminam na violação de direitos de pessoas de diferentes classes sociais situadas em toda parte do país.

Os desafios aqui apontados, juntamente com a transnacionalidade deste delito e sua propagação em massa, principalmente durante a pandemia, fez surgir o seguinte problema direcionado aos gestores do Poder Público que a presente dissertação busca responder: Será de fato que os agentes de polícia judiciária estão preparados para enfrentar a onda dos cibercrimes que vitimizam uma grande parcela da população e impõem desafios ao Estado e seus agentes?

O objetivo geral da pesquisa é analisar os delitos catalogados como virtuais e sua ofensa a bem jurídicos, propondo técnicas de investigação e apontando os desafios gerais para as polícias judiciárias.

Os objetivos específicos são: discorrer, classificar e caracterizar os delitos de internet dentro do ordenamento jurídico pátrio, sua forma de enfrentamento e quais melhores técnicas existentes para definir a autoria e comprovar a existência daqueles crimes virtuais mais habituais.

Para esta pesquisa foi levantada a seguinte hipótese: analisado as espécies de crimes digitais próprios e impróprios, especificamente, na violação dos distintos bens jurídicos, verifica-se que o aprimoramento de técnicas investigativas no âmbito da atuação investigativa, contribuirá para uma padronização de procedimento e uma uniformização das boas práticas servindo de uma poderosa frente no combate a essa espécie de delito.

Diante dessas ponderações surgiu a necessidade de reunir os crimes virtuais mais corriqueiros e se estabelecer técnicas e procedimentos padrões que possam orientar todo e qualquer representante da polícia judiciária a adotá-los quando o objetivo for identificar a autoria e a produção de elementos de informação que definam a materialidade delitiva.

Os resultados do trabalho de exame da hipótese estão expostos na presente dissertação, de forma sintetizada, como segue:

No presente trabalho, o primeiro capítulo procura demonstrar que no cometimento dos delitos de internet os infratores ofendem muito além dos diversos bens jurídicos atribuídos ao homem, alcançam a dignidade de toda e qualquer pessoa que constitucionalmente é definida como um princípio básico.

Já no capítulo seguinte, são explanadas as características, espécies, classificação, peculiaridades e adversidades dos delitos denominados de cibernéticos. Por fim, no terceiro e último capítulo, são delineados os principais desafios enfrentados pelos agentes de polícia que se debruçam com o tão falado e complexo, embora materialmente desconhecido para alguns, crimes cibernéticos. Neste mesmo sentido, se definem técnicas e medidas padrão a serem incorporadas às atividades rotineiras de polícia judiciária que visam coibir a propagação deste tipo delitivo.

O presente Relatório de Pesquisa se encerra com as Considerações Finais, nas quais são apresentados aspectos destacados da Dissertação, seguidos de estimulação à continuidade dos estudos e das reflexões sobre assunto tratado na dissertação.

Logo, o principal escopo do trabalho é apontar os desafios enfrentados pelos atores da investigação no enfrentamento dos crimes de digitais e servir como norte e ponto de partida para aqueles que se propõem a trabalhar na apuração dessa categoria delitiva.

A metodologia de pesquisa empregada foi a pesquisa analítica e bibliográfica, utilizando os métodos técnicos típicos da prática laboral do autor, como forma de trazer soluções para as hipóteses ventiladas no bojo do trabalho e de certa forma contribuir para a realidade profissional.

O Método a ser utilizado na fase de Investigação será o indutivo e método qualitativo com o uso de pesquisa bibliográfica e documental com a utilização de artigos, teses, dissertações e legislações nacionais e estrangeiras que tratam sobre o tema abordado.

CAPÍTULO 1

O PRINCÍPIO DA DIGNIDADE DA PESSOA HUMANA COMO BASE DE TUTELA DOS DISPOSITIVOS QUE ELENCAM OS CRIMES CIBERNÉTICOS

1.1 Definição e Previsão Legal dentro do Ordenamento Jurídico Brasileiro

A diversidade de delitos previstos no Código Penal Brasileiro e nas variadas e numerosas leis especiais tem sempre o mesmo objetivo final que é a proteção de bens jurídicos. Não importa qual escopo do artigo, sempre será tutelado algum direito que direta, ou na sua forma secundária, dirá respeito ao ser humano.

Da mesma forma que ao destacar os crimes digitais e a sua essência protetiva, seguirão eles o mesmo viés, proteger os direitos do indivíduo. Dificilmente se conseguirá desvincular o leque de proteção dos vários bens jurídicos da tutela principal que é a garantia da dignidade da pessoa humana.

Em primeiro plano, é de grande valia discorrer algumas considerações sobre a dignidade, por isso na visão de Silva[1]:

> "... decorre da própria natureza, o ser humano deve ser tratado sempre de modo diferenciado em face da sua natureza racional. É no relacionamento entre as pessoas e o mundo exterior e entre o Estado e a pessoa que se exteriorizam os limites da interferência no âmbito desta dignidade. (...) inexiste uma específica definição para a dignidade humana, porém ela se manifesta em todas as pessoas, já que cada um, ao respeitar o outro, tem a visão do outro. A dignidade humana existe em todos os indivíduos e impõe o respeito mútuo entre as pessoas, no ato da comunicação, e que se opõe a uma interferência indevida na vida privada pelo Estado. Tais direitos são inerentes, porque conhecidos pelas pessoas, não podendo, portanto, o Estado desconhecê-los."

Com maestria, o doutrinador Perez Luño[2] atribui que a dignidade da pessoa humana:

> "... representa um conjunto de garantias positivas e negativas. Garantias negativas no sentido de que o ser humano não pode ser objeto de discriminações e humilhações, e positivas relativamente à

---

[1] SILVA, Marco Antônio Marques da. **Acesso à justiça penal e estado democrático de direito**. São Paulo: Juarez de Oliveira, 2001.

[2] PEREZ LUÑO, Antonio Henrique. **Derechos Humanos, estado de derecho y constitucíon**. Madrid: Tecno, 2003.

> garantia de pleno desenvolvimento das suas capacidades individuais"

Já colocando a dignidade como princípio, Soares[3], define:

> "Pode-se afirmar que o princípio ético-jurídico da dignidade da pessoa humana importa o reconhecimento e tutela de um espaço de integridade físico-moral a ser assegurado a todas as pessoas por sua existência ontológica no mundo, relacionando-se tanto com a manutenção das condições materiais de subsistência quanto com a preservação dos valores espirituais de um indivíduo que sente, pensa e interage com o universo circundante."

Ao mencionar a dignidade da pessoa humana como princípio, salutar não se olvidar da função do princípio dentro de um arcabouço legislativo. Logo, buscando esclarecer sua real função, Silva e Zeni[4] atribuem que os princípios:

> "... se apresentam como instrumentos de solução no caso da existência de espaços (lacunas) deixados pelo legislador na ação de originar leis, bem como nas situações de conflitos reais entre normas que se encontram em mesmo nível hierárquico e entre os próprios princípios dotados de carga valorativa."

É na observância do conceito acima descrito pelos autores Silva e Zeni que no momento de colisão entre direitos ou mesmo entre princípios constitucionalmente postos, os agentes da polícia judiciária irão requerer, em alguns momentos, relativizar certos direitos dos investigados para possibilitar a garantia de um bem ainda maior. Por conseguinte, haverá em específicas oportunidades o dualismo entre o bem jurídico do investigado e aquele referente ao da vítima. Neste momento, entra em cena o princípio da dignidade da pessoa humana garantindo que o direito da vítima será socorrido pelos aplicadores da lei, incluindo nesse rol, os agentes investigativos.

Posto isso, constata-se a importância do citado princípio constitucional que será utilizado como instrumento na defesa daqueles situados no polo passivo dos crimes. Figurando na base de proteção a defesa da dignidade, atributo de todo ser humano.

---

[3] SOARES, Ricardo Maurício Freire. **O princípio da dignidade da pessoa humana**: em busca do direito justo. São Paulo: Saraiva, 2010.

[4] SILVA, Elizabet Leal da. ZENI, Alessandro Severino Vallér. **Algumas considerações sobre o Princípio da Dignidade da Pessoa Humana**. Revista Jurídica Cesumar – Mestrado, v.9, n.1, jan/jun 2009 – ISSN1677-6402.

Vale lembrar que a Constituição[5] Federal Brasileira, promulgada em 1988, elenca no seu rol, mais precisamente no inciso III do Art. 1º, a dignidade da pessoa humana como fundamento a ser seguido pela República Federativa do Brasil, como se pode verificar *in verbis*

TÍTULO I
DOS PRINCÍPIOS FUNDAMENTAIS

> Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos:
>
> I - a soberania;
>
> II - a cidadania;
>
> III - a dignidade da pessoa humana;
>
> IV - os valores sociais do trabalho e da livre iniciativa; (Vide Lei nº 13.874, de 2019)
>
> V - o pluralismo político.
>
> Parágrafo único. Todo o poder emana do povo, que o exerce por meio de representantes eleitos ou diretamente, nos termos desta Constituição.

Como bem preceitua Barretto[6]:

> "Ao elencar a dignidade da pessoa humana como um dos fundamentos do Estado brasileiro, a Constituição está indicando que a dignidade é o parâmetro orientador de todas as condutas estatais, o que implica romper com um modelo patrimonialista de ordem jurídica."

Ainda na mesma esteira, Barretto[7] atribui que:

> "A positivação da dignidade da pessoa humana como fundamento do Estado brasileiro impôs uma releitura, de toda, a ordem jurídica, atingindo todos os sub-ramos do Direito, que tiveram que ser rediscutidos a partir da ótica da proteção à pessoa."

Visando completar o raciocínio reverenciado, Ascenção[8] preleciona:

---

[5] Constituição Federal Brasileira.. http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 03.10.2022.
[6] BARRETTO, Rafael. **Direitos Humanos**. Juspodium: Salvador, 2022.
[7] BARRETTO, Rafael. **Direitos Humanos**. Juspodium: Salvador, 2022

> "... não podemos esquecer que a própria Constituição aponta a dignidade da pessoa humana como base da República (juntamente com a vontade popular) logo no art.1º. Dá-lhe assim, um relevo particularíssimo, pois todos os restantes preceitos constitucionais lhe estariam subordinados no ponto de vista substancial..."

Ao estabelecer a dignidade como fundamento, o legislador pretende que o Estado Brasileiro tenha como ponto de partida o respeito a este princípio que aponta como base de sustentação para a Carta Magna e também ao ordenamento jurídico brasileiro. No entanto, necessário se fazer algumas considerações desse fundamento como princípio norteador e basilar para os demais princípios presentes na carta constitucional.

Na visão dos autores Silva e Zeni[9]:

> "o princípio da dignidade da pessoa humana na Constituição Federal representa o princípio balizador dos demais princípios norteadores da Carta Magna, visto que se manifesta no sentido de mantença por parte do poder estatal dos preceitos qualitativos que permeiam a vida humana com qualidade."

Também tecendo algumas ponderações sobre como o destacado princípio é visto dentro do direito brasileiro e na própria Constituição pátria, Soares[10] retrata:

> "No ordenamento jurídico brasileiro, o princípio constitucional da dignidade da pessoa humana se desdobra em inúmeros outros princípios e regras constitucionais, confirmando um arcabouço de valores e finalidades a ser realizadas pelo Estado e pela sociedade civil, como forma de concretizar a multiplicidade de direitos fundamentais, expressos ou implícitos, da Carta Magna brasileira e, por conseguinte, da normatividade infraconstitucional derivada."

Em destaque, foi possível extrair que a dignidade da pessoa humana como princípio constitucional ascende à posição de balizador de outros princípios dentro da Constituição Pátria, servindo como importante recurso de acesso para os

---

[8] ASCENÇÃO, J. O. **A dignidade da Pessoa e o Fundamento dos Direitos Humanos**. Revista da Faculdade de Direito da Universidade de São Paulo, v.103, 2008. Disponível em: https: //www.revistas.usp.br/rfdusp/article/views/67806. Acesso em 10.07.2022.

[9] SILVA, Elizabet Leal da. ZENI, Alessandro Severino Vallér. **Algumas considerações sobre o Princípio da Dignidade da Pessoa Humana**. Revista Jurídica Cesumar – Mestrado, v.9, n.1, jan/jun 2009 – ISSN1677-6402.

[10] SOARES, Ricardo Maurício Freire. **O princípio da dignidade da pessoa humana**: em busca do direito justo. São Paulo: Saraiva, 2010.

atores da esfera investigativa no combate aos crimes digitais que afetam direitos relacionados ao ser humano. Na lacuna da lei ou no conflito entre diferentes princípios, o da dignidade da pessoa humana aparece como o solucionador dos problemas, sendo de tal maneira importante que dentre os fundamentos da Republica Federativa do Brasil figura dentro do seu rol como um dos seus pontos chaves.

1.2 A Dignidade da Pessoa Humana como Direito Fundamental

Como já explanado, a dignidade vem elencada no texto constitucional como princípio base, entretanto tal importância a ser dada pelo legislador constituinte carece de melhor explicação para possível compreensão, uma vez que também é considerado um direito fundamental.

Na concepção de Sarlet[11] a melhor definição a ser dada para a dignidade seria:

> "...como qualidade intrínseca da pessoa humana, é irrenunciável e inalienável, constituindo elemento que qualifica o ser humano como tal e dele não pode ser destacado (...). Nessa trilha, compreendida como qualidade integrante e irrenunciável da própria condição humana, a dignidade pode (e deve) ser reconhecida, respeitada, promovida e protegida, não podendo, contudo (no sentido ora empregado) ser criada, concedida ou retirada (embora possa ser violada) já que reconhecida e atribuída a cada ser humano, que, não sendo indispensável, é insubstituível..."

Buscando firmar uma clara compreensão sobre a dignidade da pessoa humana, Soares[12] leciona que:

> "... antes mesmo de seu reconhecimento jurídico nas Declarações Internacionais de Direito e nas Constituições de diversos países, figura como um valor, que brota da própria experiência axiológica de cada cultura humana, submetida aos influxos do tempo e do espaço."

Comparato[13] adjetiva a dignidade como transcendente e na visão do ilustre autor:

---

[11] SARLET, Ingo Wolfang. **Dignidade (da Pessoa) Humana e Direitos Fundamentais na Constituição de 1988**. Porto Alegre: Livraria do Advogado Editora, 2015.
[12] SOARES, Ricardo Maurício Freire. **O princípio da dignidade da pessoa humana**: em busca do direito justo. São Paulo: Saraiva, 2010.

> "... é um atributo essencial do homem enquanto pessoa, isto é, do homem em sua essência, independentemente das qualificações específicas de sexo, raça, religião, nacionalidade, posição social ou qualquer outra."

No sentido de atribuir a verdadeira importância que o citado direito se tornou, o renomado constitucionalista José Afonso da Silva[14] salienta que:

> "... a Constituição, reconhecendo a sua existência e a sua eminência transformou-a num valor supremo da ordem jurídica, quando a declara como um dos fundamentos da República Federativa do Brasil constituída em Estado Democrático de Direito."

A real intenção do legislador constituinte em introduzir o princípio da dignidade da pessoa humana no bojo da Constituição Federal de 1988 foi estabelecer e, de certa forma, consagrá-lo como princípio matriz diante de outros, também considerados fundamentais, dentro do próprio texto. Sendo inerente a todo indivíduo, ao qual não poderá dispor e sempre poderá ser sustentado na defesa da sociedade.

Sarlet[15], ao observar uma diversidade de definições sobre a dignidade da pessoa humana e seus motivos que o elevam, a tal importância, ao ponto de ser considerado um direito fundamental exposto na Carta Magna, atribui como um completo conceito:

> "... a qualidade intrínseca e distintiva reconhecida em cada ser humano que o faz merecedor do mesmo respeito e considerável por parte do Estado e da comunidade, implicando, neste sentido, um complexo de direitos e deveres fundamentais que assegurem a pessoa tanto contra todo e qualquer ato de cunho degradante e desumano, como venham a lhe garantir as condições existenciais mínimas para uma vida saudável, além de propiciar e promover sua participação ativa e corresponsável nos destinos da própria existência e da vida em comunhão com os demais seres humanos, mediante o devido respeito aos demais seres que integram a rede da vida."

---

[13] COMPARATO, Fábio Konder. **Fundamento dos Direitos Humanos**. Revista O tempo em Movimento, edição 36, nº 3, 2017.
[14] SILVA, José Afonso da. **A dignidade da Pessoa Humana como valor supremo da democracia**. Revista do Direito Administrativo. nº212, abr/jun. Rio de Janeiro, 1998.
[15] SARLET, Ingo Wolfang. **Dignidade (da Pessoa) Humana e Direitos Fundamentais na Constituição de 1988**. Porto Alegre: Livraria do Advogado Editora, 2015.

Diante do que foi exposto, válido destacar que na medida em que surge necessidade de resguardar ao ser humano o mínimo de condições básicas para sua sobrevivência, aparece a dignidade da pessoa humana como garantia. Assim sendo, pode-se dizer que figura como direito fundamental inerente à todos, capaz de ser acionado caso haja ofensa aos elementos mínimos que impeçam alguém de ter uma vida normal. Podendo buscar socorro ao Poder Judiciário alegando uma grave violação a sua condição digna de sobrevivência, ou seja, desrespeito a um direito fundamental.

É nessa linha de pensamento que também se busca a proteção das vítimas dos cybercrimes, pois mesmo sem uma previsão expressa de crime para determinada conduta ofensiva à um bem jurídico de alguém, é sobre a alegação de violação da dignidade da pessoa humana, como direito fundamental, que se baseiam os operadores do direito na justificação jurídica de uma medida cautelar de urgência para salvaguardar o direito de uma pessoa na posição de vítima.

1.3 A ofensa aos diversos bens jurídicos no cometimento dos crimes de internet em paralelo com o desrespeito à dignidade da pessoa humana

Na observância dos delitos ditos como virtuais, há previsão deles em algumas leis especiais, como o Estatuto da Criança e do Adolescente, por exemplo, como também em variadas passagens dentro do Código Penal. Contudo, na proporção em que a sociedade condiciona ainda mais suas atividades à tecnologia e ao uso da internet, aumenta a sua vulnerabilidade e sujeição aos delitos digitais.

A chegada da tecnologia 5G, veio como facilitadora do dia dia das pessoas e elemento atrativo para o mundo virtual. O maior tempo disponível na rede de computadores, amplia consideravelmente o número dessa especificidade delitiva e, associado a isso, cresce também os ataques aos bens jurídicos.

Em linhas gerais, nota-se que há uma frequente violação aos bens jurídicos honra, patrimônio, dignidade sexual, liberdade sexual, incolumidade física, privacidade e intimidade. Entretanto, sem querer esgotar todos os direitos ofendidos, pode-se afirmar que as violações a estes arroladas são as mais corriqueiras dentro da esfera de ocorrências registradas na polícia judiciária.

Falar de todos esses direitos, jamais pode ser deixado de lado a dignidade da pessoa humana que é a base de tudo. Já que alguém que, por exemplo, tem a sua dignidade sexual desrespeitada, também será afetada a sua condição digna de viver. Logo, todos os objetos jurídicos voltados para o indivíduo estão, de alguma forma, interligados com o direito fundamental que figura na base de todos eles, qual seja, a dignidade da pessoa humana.

Segundo essa linha de raciocínio, Masson[16] pontua e exemplifica:

> "... toda e qualquer pessoa humana tem o direito de exigir respeito no âmbito da sua vida sexual, bem como de respeitar as opções sexuais alheias. O Estado deve assegurar meios para todos buscarem a satisfação sexual de forma digna, livre de violência, grave ameaça ou exploração."

O Estado Brasileiro não só considerou a dignidade da pessoa humana como fundamento, mas também dentro do seu corpo constitucional a elevou a objetivo a ser alcançado por todos aqueles zeladores do ordenamento jurídico nacional.

De maneira didática, para uma melhor afirmação do exposto anteriormente, o autor Barretto[17] destaca:

> "Os objetivos fundamentais do Estado constituem os pontos em que o Estado pretende chegar, e, no caso brasileiro, eles estão diretamente relacionados com a dignidade da pessoa, a revelar, mais uma vez, o compromisso do constituinte com a busca da proteção à pessoa."

No mesmo sentido, Barretto continua esclarecendo:

> "..., no art. 3º, ao elencar os objetivos fundamentais do Estado brasileiro, a Constituição novamente denotou preocupação em afirmar a dignidade da pessoa humana, pois todos os objetivos estão relacionados com a busca da dignidade da pessoa humana."

Portanto, na defesa daqueles que são vítimas dos, cada vez, mais frequentes, crimes virtuais, não só caberá apontar a ofensa ao objeto jurídico específico, já que conectado a este estará sempre a dignidade do ser humano, direito fundamental constitucional.

---

[16] MASSON, Cleber. **Direito Penal Esquematizado, vol.3: parte especial**. Método: São Paulo, 2013.
[17] BARRETTO, Rafael. **Direitos Humanos**. Juspodium: Salvador, 2022.

De certa forma, no combate aos delitos digitais e suas inúmeras violações aos direitos das pessoas, tanto é dever do Estado atacar a nova e crescente espécie de crime, como necessitam os agentes públicos, que agem no cumprimento da lei, ter como enfoque o respeito a todo e qualquer direito básico do homem.

1.4 O princípio da dignidade da pessoa humana como escopo máximo de proteção da legislação que estabelece os crimes digitais

Em tempos atuais, basta observar algumas notícias em periódicos digitais, ou mesmo televisivas, para se deparar com algum tipo de crime virtual. Dentro da era 4.0 da tecnologia, a utilização ainda maior da tecnologia coloca os usuários às margens do limite de segurança e suscetíveis a sofrerem ataques pelos criminosos digitais.

Mesmo que o legislador infraconstitucional atribua em determinado tipo penal a proteção a um direito atrelado ao ser humano, sempre pretenderá como escopo máximo a dignidade da pessoa, ou seja, os direitos humanos, em linhas gerais.

Os direitos humanos estão como gênero da espécie dignidade do indivíduo e, nesse sentido, a autora Soares18 salienta que estes "são, então, naturais, universais, históricos e, também, indivisíveis e interdependentes porque à medida que são acrescentados ao rol dos direitos fundamentais da pessoa humana eles não podem ser mais fracionados".

Na mesma esteira, pontua Ferreira, Zenaide e Náder19 que os direitos humanos:

> "... são aqueles princípios ou valores que permitem a uma pessoa afirmar sua condição humana e participar plenamente da vida. (...) se aplicam a todos os homens e servem para proteger a pessoa de tudo que possa negar sua condição humana. Com isso, eles aparecem como um instrumento de proteção do sujeito contra todo tipo de violência (...) servem, assim, para assegurar ao homem o exercício da liberdade, preservação da dignidade e a proteção da sua

[18] SOARES, Maria Victoria de Mesquita Benevides. **Cidadania e Direitos Humanos**. Revista Cadernos de Pesquisa, vol. 45. Fundação Carlos Chagas:2014.
[19] FERREIRA, Lúcia de Fátima Guerra; ZENAIDE, Maria de Nazaré Tavares; NÁDER, Alexandre Antônio Gili; **Educando em Direitos Humanos**: fundamentos histórico-filosófico e políticos jurídicos. Editora da UFPB: João Pessoa, 2016.

> existência. (...) Eles são essenciais à conquista de uma vida digna, daí serem considerados fundamentais à nossa existência..."

Estabelecendo ainda uma conexão entre direitos humanos e dignidade da pessoa, Ascenção[20] discorre:

> "A pessoa, repisamos, tem dignidade porque é pessoa. Os direitos humanos que se lhe reconhecem têm como fundamento essa dignidade, provinda da capacidade de auto-realização da personalidade..."

Visando conferir merecido destaque ao ponto fulcral de alicerce a todo e qualquer crime, Masson[21] disserta:

> "... a dignidade é inerente a todas as pessoas, sem qualquer distinção, em decorrência da condição privilegiada do ser humano. Ademais, a dignidade da pessoa humana não gera reflexos apenas nas esferas física, moral e patrimonial, mas também no âmbito sexual..."

Silva[22] destaca que a dignidade da pessoa humana:

> "... constitui um valor que atrai a realização dos direitos fundamentais do homem, em todas as suas dimensões, e, como a democracia é o único regime político capaz de propiciar a efetividade desses direitos, o que significa dignificar o homem, é ela que se revela como o seu valor supremo, o valor que a dimensiona e humaniza."

Todo qualquer delito virtual viola direito atrelado ao homem, que tem como base fazer parte de um rol que corresponde à dignidade de todos os indivíduos e de maneira ampla se coligam aos direitos humanos. Assim, um é incorporado ao outro, mas tudo precisa ser tutelado pelo Estado e a forma que é exposta na constituição brasileira garante uma aplicabilidade imediata.

Elevando o Estado à posição de garantidor e vinculando a busca da dignidade à justiça, os autores Silva e Zeni[23] defendem que "é primordial o

---

[20] ASCENÇÃO, J. O. **A dignidade da Pessoa e o Fundamento dos Direitos Humanos**. Revista da Faculdade de Direito da Universidade de São Paulo, v.103, 2008. Disponível em: https: //www.revistas.usp.br/rfdusp/article/views/67806. Acesso em 10.07.2022.
[21] MASSON, Cleber. **Direito Penal Esquematizado, vol.3: parte especial**. Método: São Paulo, 2013
[22] SILVA, José Afonso da. **A dignidade da Pessoa Humana como valor supremo da democracia**. Revista do Direito Administrativo. nº212, abr/jun. Rio de Janeiro, 1998.

entendimento de que a proteção ao homem é que remete ao atendimento do princípio da dignidade da pessoa humana, uma vez que a dignidade está intimamente relacionada à justiça".

Na mesma ideia de justiça atribuída ao princípio da dignidade da pessoa humana como direito fundamental, Soares[24] elenca que esse princípio

> "...permite reconstruir o modo de compreensão e aplicação dos direitos fundamentais no sistema jurídico brasileiro, potencializando a realização de justiça ao oportunizar a aceitação da aplicabilidade direta e imediata dos direitos fundamentais..."

Por mais que tente destacar algum crime cometido por intermédio da internet, vindo a denegrir, por exemplo, o patrimônio, a honra ou a liberdade sexual, restou clarividente que não existe forma de afastar o objetivo maior de um delito positivado na lei pátria. A dignidade da pessoa humana, seja como espécie dos direitos humanos, ou mesmo ligado à ideal de justiça, será sempre um fundamento constitucional posto no texto magno que todo e qualquer cidadão deve reivindicar quando ocorra o seu desrespeito.

Na medida em que é vinculado a toda e qualquer pessoa, a mencionada dignidade não poderá ser tolhida, retirada ou reduzida, não importa a espécie de infração penal praticada, estará ela na base de tutela de todas as infrações, inclusive, dos crimes cibernéticos.

---

[23] SILVA, Elizabet Leal da. ZENI, Alessandro Severino Vallér. **Algumas considerações sobre o Princípio da Dignidade da Pessoa Humana**. Revista Jurídica Cesumar – Mestrado, v.9, n.1, jan/jun 2009 – ISSN1677-6402.

[24] SOARES, Ricardo Maurício Freire. **O princípio da dignidade da pessoa humana**: em busca do direito justo. São Paulo: Saraiva, 2010.

CAPÍTULO 2

DOS CRIMES CIBERNÉTICOS

2.1. O Início de uma Nova Era – A Era Digital

Os avanços tecnológicos advindos da 3ª Revolução Industrial transformaram o Século XXI na nova era denominada de Era Digital. Período ao qual o uso cada vez mais frequente de computadores, ainda mais rápidos com seus super processadores, proliferou com a criação de dispositivos móveis conhecidos como smartphones. Esses pequenos dispositivos quase como mini computadores, devido às suas multifunções popularizaram o acesso das pessoas à internet.

No intuito de esclarecer melhor a importância e funcionalidade de um smartphone, Zaniolo[25] estabelece:

> "Smartphone ou telefone inteligente pode ser definido como aparelho telefônico móvel com funcionalidades de assistente digital pessoal (PDA) e recursos básicos de computadores pessoais, como correio eletrônico (e-mail) e navegação na web. Tal arranjo permite que seja utilizado de forma independente (como telefone comum ou PDA), tornando-se, com a combinação dessas duas características, poderosa ferramenta para a troca de dados, imagens e uma variedade de formatos de arquivo, com outros dispositivos e computadores."

Para Crespo[26] essa nova era é definida como a "Era da Informação" e segundo ele:

> "Comumente se conhece a Era da Informação como o período após a Era Industrial, principalmente após a década de 1980, apesar de suas bases fundarem-se no início do século XX, especialmente na década de 1970, com as invenções do microprocessador, das redes de computadores, da fibra ótica e do computador pessoal."

Nos tempos atuais, a internet deixou de ser somente um ambiente de coleta de informações, passando a servir como fonte de entretenimento, ensino e até ferramenta de trabalho. A gama de produtos e serviços disponíveis atraiu uma

---

[25]ZANIOLO, Pedro Augusto. **Crimes Modernos**: Os impactos da Tecnologia no Direito. Salvador: Editora JusPodium, 2021.
[26] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011.

grande quantidade de pessoas que submetem quase 2/3 do seu tempo conectados à internet através de computadores ou dispositivos móveis.

Desde o surgimento da web, ou seja, ao passar de décadas, pode-se dizer que existem gerações de acesso à ela, algumas tiveram que passar por um processo de adaptação e inseri-la na sua rotina, outros somente a aderiram tardiamente, enquanto os mais modernos já nasceram com a sua existência e não sabem o que é conviver sem a participação dela nos seus diversos aspectos. Como melhor forma de definir essas distintas gerações, Palfrey e Gasser[27] discorrem que a era digital:

> "...transformou o modo como as pessoas vivem e se relacionam umas com as outras e com o mundo que os cerca. Algumas pessoas mais velhas estavam ali no início, os colonizadores digitais não nativos do ambiente virtual, porque cresceram em um mundo apenas analógico ... Outras estão menos familiarizados com esse ambiente, os Imigrantes Digitais, que aprenderam tarde na vida a mandar e-mails e usar as redes sociais."

Os mesmo autores, Palfrey e Gasser[28] definem a geração que nasceu dentro do ciclo virtual como nativos digitais e estes:

> "passam grande parte da vida online, sem distinção entre o online e o offline. Em vez de pensarem na sua identidade digital e em sua identidade no espaço real como coisas separadas, eles têm apenas uma identidade... São unidas por um conjunto de práticas comuns, incluindo a quantidade de tempo que passam usando tecnologias digitais, sua tendência para as multitarefas, os modos como se expressam e se relacionam uns com os outros de maneiras medievas pelas tecnologias digitais."

Na medida em que aumenta o número de serviços disponíveis e a relação de exposição das pessoas quanto ao seu tempo e vidas privadas, ampliam a vulnerabilidade destes à nova espécie de criminosos responsáveis pela prática de crimes cibernéticos.

Fatores como o aumento do tempo e do acesso à internet, a ampliação do trabalho *home office*, a adaptação das aulas para plataformas *on line* e o frequente acesso às redes sociais, são suficientes para a ampliação da suscetibilidade aos

---

[27] PALFREY, John. GASSER, Urs. **Nascidos na Era Digital** – Entendendo a Primeira Geração de Nativos Digitais. Ed Artmed. Porto Alegre, 2011.
[28] Idem

crimes digitais. Diante disso, os delitos virtuais cresceram não só na quantidade, mas também na variabilidade e sofisticação.

Além disso, aqueles definidos como “nativos digitais” pela dependência de desenvolver suas atividades somente perante a rede mundial de computadores passam a relaxar quanto às precauções necessárias pelo uso excessivo deste recurso que por um lado tornam suas vidas mais práticas, entretanto por outro lado as expõem ainda mais aos riscos dos criminosos virtuais. Nessa mesma linha de pensamento, Palfrey e Gasser[29] preconizam:

> “... muitas das mudanças na maneira em que os Nativos Digitais vivem suas vidas são motivos de preocupação. Por exemplo, eles têm ideias com relação à privacidade diferentes daquelas das gerações anteriores. No processo de passar tempo demais nesse ambiente de conexão digital, eles estão deixando mais vestígios de si mesmos nos locais públicos online... A cada hora que passam conectados online, estão deixando mais rastros para os marqueteiros – e também os pedófilos – seguirem... A repercussão destas mudanças, nas próximas décadas, será profunda para todos nós. Mas aqueles que estão crescendo como Nativos Digitais estão em vias de pagar o preço mais alto.”

A maior propensão desse seleto grupo aos ataques virtuais passa também pela expansão da conectividade trazida pela globalização. Este último tem grande influência no surgimento dessa nova modalidade delitiva (Crimes digitais), tendo em vista que foi através dos avanços tecnológicos e da quebra de fronteiras espaciais que as pessoas puderam ter um maior acesso às redes e à internet.

A transnacionalidade desses crimes cresceu em um ritmo tão acelerado que foi necessário uma mobilização mundial para propor uma legislação comum entre os países. Neste sentido, diversas nações se uniram na Convenção de Budapeste com esse e outros propósitos para o combate aos cibercrimes.

De uma forma ou de outra, a nova era digital veio para fazer parte da vida de todos e necessário é adaptar-se a ela, como forma de usufruir dos seus benefícios, mas também prevenir-se dos seus malefícios. Dentre eles, se pode dizer que está o crime digital, que atingirá um numeroso quantitativo de pessoas em

[29] PALFREY, John. GASSER, Urs. **Nascidos na Era Digital** – Entendendo a Primeira Geração de Nativos Digitais. Ed Artmed. Porto Alegre, 2011.

diferentes espaços do globo terrestre e a web se tornará o campo vasto e propício para essa nova escalada criminosa.

2.2 Dos crimes Cibernéticos

A era digital trouxe também à baila uma imensidão de ações envolvendo pessoas. Por um lado trouxe praticidade às coisas, encurtou distâncias e ampliou a comunicação entre indivíduos de diferentes lugares do globo. Todavia, por outro lado, a tecnologia criou novos mecanismos de prática de crimes, através dos quais delitos são praticados por intermédio da internet, ou mesmo, surgiram por causa dela, configurando-se como novos crimes que emergiram dentro de um novo ordenamento jurídico.

Para Barreto[30], os crimes cibernéticos "são aqueles que envolvem o uso de tecnologias (computador, internet, caixas eletrônicos), sendo, em regra, crimes meios – ou seja, apenas a forma em que são praticados é que é inovadora".

Já Darós Malaquias[31] define delito informático como a conduta:

> "típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com ou sem 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 confiabilidade."

Na visão do ilustre autor Cassanti[32]:

> "toda a atividade onde um computador ou uma rede de computadores é utilizada como ferramenta, base de ataque ou como meio de crime é conhecido como cibercrime. Outros termos que se referem a essa atividade são: crime informático, crimes eletrônicos, crime virtual ou crime digital".

A fraude criminosa pode derivar de falsos e-mails, envio de links falsos, instalação indevida de softwares, criação de perfis falsos, entre outros. No entanto,

---

[30] BARRETO, Alessandro Gonçalves/Brasil, Beatriz Silveira. **Investigação Cibernética,** à luz do Marco Civil da Internet. Rio de janeiro. Brasport, 2016, p.16.
[31] DARÓS MALAQUIAS, Roberto Antônio. **Crime Cibernético e Prova,** investigação criminal em busca da verdade. Curitiba. Editora Juruá, 2015, p.38
[32] CASSANTI, Moisés de Oliveira. **Crimes Virtuais – vítimas reais.** Rio de Janeiro. Brasport, 2014.

pela grande acessibilidade aos meios digitais é perceptível que o perfil dos criminosos virtuais não é mais aquele do exímio conhecedor do sistema informático, agora, ainda mais, depara-se com pessoas comuns que se utilizam da rede mundial de computadores para prática criminosa, como por exemplo, a crescente onda dos delitos contra a honra usando perfis falsos, aos quais pessoas se passam por outras e cometem os delitos de falsa identidade, calúnia, difamação e, principalmente, injúria.

Nessa esteira, corrobora Cassanti[33], em explanar que:

> o maior incentivo aos crimes virtuais é dado pela falsa sensação de que o meio digital é um ambiente sem leis, mas é importante saber que quando o computador é uma ferramenta para prática dos delitos, suscita a possibilidade de se amoldar aos tipos penais já existentes.

O crescimento exponencial da quantidade de delitos em números e espécies não abrange na mesma proporcionalidade o número de procedimentos policiais e punições por este tipo de delito. A legislação ainda é muito branda ou falha, pois por um lado atribui a certos tipos de condutas penas irrelevantes, já por outro não aborda as ações praticadas, ou seja, explicitam uma nítida lacuna jurídica que deixa os infratores à margem da lei.

Ações muito corriqueiras como as ofensas entre pessoas que utilizam as redes sociais, são de significativo crescimento pela falsa percepção dos usuários em achar que o ambiente virtual é um campo sem lei, talvez motivadas pelas reduzidas penas. Contudo existem atos criminosos bastante comuns como a propagação de vírus, seja para causar dano à patrimônio de outrem, seja para tentar colher ilicitamente informações, com nova previsão no ordenamento jurídico brasileiro, ainda pouco difundida e aplicada, talvez pela ausência de conhecimento técnico que contribua para deixar este novo delito dentre do rol daqueles que fazem parte dos inquéritos policiai.

Nessa linha de raciocínio Cassanti[34] afirma que:

> Para o Judiciário, 95% dos delitos cometidos eletronicamente estão tipificados no Código Penal brasileiro por caracterizarem crimes

[33] CASSANTI, Moisés de Oliveira. **Crimes Virtuais – vítimas reais.** Rio de Janeiro. Brasport, 2014
[34] CASSANTI, Moisés de Oliveira. **Crimes Virtuais – vítimas reais.** Rio de Janeiro. Brasport, 2014.

> comuns praticados através da internet. Os outros 5% para os quais faltaria enquadramento jurídico abrangem transgressões que só existem no mundo virtual, a exemplo da distribuição de vírus eletrônico e dos ataques DDoS.

2.2.1. Os crimes cibernéticos propriamente ditos

Com o passar do tempo, não só os direitos individuais eram de certa forma afetados, como a sociedade moderna trouxe consigo um inumerado de ações que atingem direitos coletivos levando a uma amplitude de atuação do direito penal. Sendo assim, é possível acrescer que o Direito Penal Moderno assume um papel ainda mais protetor diante de diversas novas condutas ofensivas a bens jurídicos que necessitam de tutela.

A necessidade que surge com a evolução da sociedade exige do legislador a adoção de uma dogmática mais contemporânea e atrelada às mudanças temporais como forma de acompanhar o dinamismo social, criando assim novos tipos penais e promovendo a punição de novos atos.

Certos atos originários dos novos tempos, pela sua atipicidade permitem que criminosos praticantes destes atos violadores atuem livremente e por isso precisam ser tolidos para evitar que a sensação de impunidade das suas condutas se propague negativamente e seja um incentivo para novos infratores.

É dentro deste cenário que surge a positivação dos crimes virtuais próprios. O desconhecimento do legislador e as novas práticas criminosas utilizando mecanismos nunca antes visto que exige dele uma adequação à realidade da sociedade.

Diante disso, torna-se necessário a introdução de novas condutas que atingem direitos individuais e coletivos no ordenamento jurídico brasileiro. Assim surge a lei Caroline Dieckmann, lei 12.737/12, que elenca algumas ações específicas que simbolizam crimes digitais e que pela sua frequente ocorrência carecia de uma codificação para posterior punição dos criminosos virtuais.

Portanto, necessário se faz tecer uma classificação dos delitos virtuais podendo estes ser divididos como puros ou próprios e também como impuros ou impróprios. Na visão de Barreto[35], puros ou próprios são:

> "...aqueles em que os sistemas informatizados, banco de dados, arquivos ou terminais (computadores, smartphones, tablets, por exemplo) são atacados pelos criminosos, normalmente após a identificação de vulnerabilidades, seja por meio de programas maliciosos ou, ainda, por engenharia social."

Destarte, essa nova categoria delitiva difere daquelas já existentes e constitui um novo desafio para juristas, executores da lei e para a sociedade como um todo.

2.2.2. Delitos Virtuais Abertos

Uma vez tecido considerações sobre crimes cibernéticos próprios e impróprios, necessário se faz também abordar mais alguns elementos que contribuem para a classificação dessa modalidade delitiva e sua melhor compreensão.

Dia após dia, é perceptível nos noticiários televisivos e, principalmente dentre do ambiente de uma delegacia de polícia, como os crimes mais corriqueiros como aqueles contra a honra e o de ameaça estão cambiando para o cometimento em grande parte dentro de um cenário virtual.

Com o escopo de utilizar a internet como garantia de impunidade e também pelo dominante uso de dispositivos eletrônicos para uso pessoal, diversos delitos estão migrando de cenário físico para o virtual. Em alguns deles, os autores deixam fácil rastro e os não se preocupam em esconder-se, por outro lado outros criam perfis falsos e buscam burlar a sua real identificação.

Todavia, crimes como injúria, calúnia, difamação, ameaça, furto mediante fraude e estelionato, fazem parte de um rol de delitos que cada dia mais são praticados através da internet. Fato que amplia o desafio para as polícias judiciárias

---

[35] BARRETO, Alessandro Gonçalves/Brasil, Beatriz Silveira. **Investigação Cibernética,** à luz do Marco Civil da Internet. Rio de janeiro. Brasport, 2016.

dos Estados que precisam intensificar e utilizar técnicas específicas para coletar informações que sirvam como prova e apontem a autoria delitiva.

É nesse diapasão que autores como Wendt e Jorge[36] buscam classificar alguns dos crimes virtuais como “crimes cibernéticos abertos” e por isso definem que

> “... são aqueles que podem ser praticados da forma tradicional ou por intermédio de computadores, ou seja, o computador é apenas um meio para a prática do crime, que também poderia ser cometido sem o uso dele.”

Sem sombra de dúvidas, esses crimes virtuais abertos como acima definidos possuem tratativas bem distintas dentro do âmbito de uma delegacia de polícia quando comparados com a sua forma tradicional. Este último, costuma ter maior celeridade na abertura de procedimentos investigativos, enquanto, diversamente, os virtuais não são dados a devida atenção como o caso requer, tudo indica, pelo desconhecimento de como adequadamente se deve colher informações pertinentes ao fato registrado em boletim de ocorrência.

2.2.3. Delitos exclusivamente Virtuais

Na medida em que surgem situações prejudiciais contra um grande grupo de pessoas em diferentes Estados da Federação, desde que seja constatada a atipicidade daquela conduta, o legislador pátrio, trata de inserir essa nova “engenharia” ofensiva a algum bem jurídico dentro de uma lei e a considera como delito. Assim, estabelecendo uma pena privativa de liberdade em abstrato.

Observando o ordenamento jurídico pátrio, não será possível localizar uma mudança legislativa prevendo um crime digital com muito tempo de “rodagem’’, isto porque o uso popularizado da web e o surgimento de delitos específicos não são antigos e, de certa forma, ainda carecem de instrumentos reguladores mais claros e protetores.

No entanto, o uso da internet em grande escala trouxe para o direito brasileiro uma positivação inovadora e específica. Em diferentes institutos

[36] WENDT, Emerson. JORGE, Higor Vinícius Mendonça. **Crimes Cibernéticos**: Ameaças e Procedimentos de Investigação. Rio de Janeiro. Ed. Brasport, 2013.

legislativos, como leis especiais e o código penal, apareceram delitos estritamente virtuais que passaram a exigir dos aplicadores da lei um conhecimento mais específico.

Nesta esteira, Wendt e Jorge[37] detalham que os crimes exclusivamente cibernéticos são diferentes:

> "... pois eles somente podem ser praticados com a utilização de computadores ou de outros recursos tecnológicos que permitem o acesso à internet. Um exemplo é o crime de aliciamento de crianças praticados por intermédio de salas de bate papo na internet, previsto no Art. 241D do Estatuto da Criança e do Adolescente (Lei 8.069/90). Também são exemplos os crimes de Interceptação Telemática Ilegal e o recém-aprovado crime de invasão de computadores."

Sendo exclusivamente virtuais ou virtuais abertos, a dificuldade de enfrentar as barreiras da produção de provas e identificação continuam para àqueles que militam dentro da atividade investigativa. O aparecimento de novos delitos, agora considerados estritamente virtuais, exige uma qualificação da polícia e o treinamento intensificado para não permitir uma gama delitiva dentro das cifras negras e distanciando a *novatio legis* do seu real propósito.

2.2.4. Dos crimes de internet na sua forma imprópria

Dentro do direito pátrio há uma variedade de delitos postos em legislações especiais e, na sua maioria, na estrutura do Código Penal. Na medida em que a sociedade evolui, os criminosos procuram variar na sua forma de utilizar o fator surpresa para atingir novas vítimas. É nessa ótica que surgem os crimes de internet impróprios, pois nada mais é que os crimes comuns cometidos através na rede mundial de computadores.

Barreto[38], estabelece como impuros ou impróprios:

> "...aqueles onde o dispositivo tecnológico é utilizado como meio para a prática do delito, propiciando a sua execução ou o seu resultado. Aqui apenas o veículo em que o crime é praticado é que envolve a

[37] WENDT, Emerson. JORGE, Higor Vinícius Mendonça. **Crimes Cibernéticos**: Ameaças e Procedimentos de Investigação. Rio de Janeiro. Ed. Brasport, 2013.
[38] BARRETO, Alessandro Gonçalves/Brasil, Beatriz Silveira. **Investigação Cibernética,** à luz do Marco Civil da Internet. Rio de janeiro. Brasport, 2016.

> tecnologia, sendo perfeitamente adequados diversas figuras típicas previstas no Código Penal Brasileiro ou em leis penais especiais."

O uso desse instrumento por quase toda totalidade do globo, leva o infrator a buscar adaptações aos atos considerados como típicos e o meio para práticas delitivas antigas somente ganhou nova roupagem, contudo continua atingindo os mesmos bens jurídicos atrelados ao indivíduo.

Didaticamente para melhor compreensão, Crespo[39] leciona:

> "... os crimes digitais impróprios nada mais são que aqueles já tradicionalmente tipificados no ordenamento, mas agora praticados com o auxílio de modernas tecnologias. Assim, essa denominação apenas representa que os ilícitos penais tradicionais podem ser cometidos por meio de novos *modi operandi*. Ocorre que alguns desses ilícitos ganham impressionante repercussão justamente por serem praticados por meio de ações envolvendo os meios tecnológicos."

Nos tópicos seguintes, serão ilustrados os crimes digitais impróprios mais corriqueiros nos dias atuais, analisando como eles têm dominado o cenário do registro de ocorrências dentro de uma delegacia de polícia.

2.3. Os tipos de cybercrimes impróprios de maior incidência no cenário brasileiro

Atualmente, uma parcela dos delitos tradicionais possibilita seu cometimento por intermédio da web, permitindo que criminosos atuem distante do local do crime e permita maior margem para impunidade. O elemento de distância geográfica entre autor e vítima tem possibilitado o encorajamento de pessoas a praticarem uma quantidade maior de crimes com a difícil chance de ser identificado e responsabilizado.

Observando o ordenamento jurídico pátrio, não será possível localizar uma mudança legislativa prevendo um crime digital com muito tempo de existência, isto porque o uso popularizado da rede mundial de computadores e o surgimento de

[39] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011.

delitos específicos possuem a característica de serem contemporâneos, desta forma acabam por carecer de instrumentos reguladores mais claros e protetores.

No entanto, o uso da web em grande escala trouxe para o direito brasileiro uma positivação inovadora e específica. Em diferentes institutos legislativos, como leis especiais e o código penal, apareceram delitos estritamente virtuais que passaram a exigir dos aplicadores da lei um conhecimento mais apurado.

Nesta esteira, Wendt e Jorge[40] detalham que os crimes exclusivamente cibernéticos são diferentes:

> "... pois eles somente podem ser praticados com a utilização de computadores ou de outros recursos tecnológicos que permitem o acesso à internet. Um exemplo é o crime de aliciamento de crianças praticados por intermédio de salas de bate papo na internet, previsto no Art. 241D do Estatuto da Criança e do Adolescente (Lei 8.069/90). Também são exemplos os crimes de Interceptação Telemática Ilegal e o recém-aprovado crime de invasão de computadores."

Sendo exclusivamente virtuais ou virtuais abertos, a dificuldade de enfrentar as barreiras da produção de provas e identificação continuam para aqueles que militam dentro da atividade investigativa. O aparecimento de novos delitos, agora considerados estritamente virtuais, exige uma qualificação da polícia e o treinamento intensificado para não permitir uma nova categoria delitiva dentro das cifras negra, distanciando a *novatio legis* do seu real propósito.

2.3.1. Invasão de Dispositivo Informático

No ano de 2012, foi promulgada a *novatio legis* incriminadora, denominada de Lei Carolina Dieckmann, Lei n° 12.737. A motivação para a proposição legislativa frente ao Congresso Nacional ocorreu devido a invasão ao computador da atriz Carolina Dieckmann por um criminoso que conseguiu lograr êxito em obter fotos sensuais dela e posteriormente passou a exigir dinheiro para não divulgar o material adquirido furtivamente.

---

[40] WENDT, Emerson. JORGE, Higor Vinícius Mendonça. **Crimes Cibernéticos**: Ameaças e Procedimentos de Investigação. Rio de Janeiro. Ed. Brasport, 2013.

De forma analítica, o autor Estefam[41] traça um panorama sobre o escopo da criação da Lei 12.737/12, ao qual, segundo ele:

> "Havia, porém, uma considerável gama de comportamentos ilícitos praticados no ambiente informatizado que se mostravam atípicos e, em virtude da proibição de analogia *in malam partem*, não poderiam ser açambarcados pelo manto protetivo do Direito Penal, senão por meio de uma reforma legislativa. A Lei n. 12.737/2012 foi elaborada justamente com este escopo, ou seja, muito mais do que "homenagear" uma atriz, surgiu para colmatar relevantes lacunas existentes no ordenamento jurídico. Afinal, não se punia criminalmente, até então, a instalação de vírus em computadores alheios ou o oferecimento a terceiros de programas (*softwares*) ou dispositivos capazes de realizar tais operações (comportamentos incluídos no atual art. 154-A do CP)."

O delito da Invasão de Dispositivo eletrônico, criado pela lei ordinária citada, teve o seu texto fixado no Código Penal, mais precisamente no Art. 154A[42], prevendo como comportamento punitivo a invasão em dispositivo informático de forma clandestina, ou seja, sem a autorização do usuário. Desta forma, de acordo com o texto legal:

> "Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita:
>
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, 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 1/3 (um terço) a 2/3 (dois terços) 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 2 (dois) a 5 (cinco) anos, e multa

---

[41] ESTEFAN, André. **Direito Penal**: Parte Especial – Arts. 121 a 234-C – v. 2. São Paulo : SaraivaJur, 2022.

[42] **CÓDIGO PENAL BRASILEIRO**, https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm, acesso em 17/12/2022.

> § 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."

Há o escopo de tutelar a segurança informática, que nada mais é do que garantir uma navegação na rede internet com seus dados pessoais preservados. Enfim, visa proteger a intimidade do usuário, na medida em que deseja a inviolabilidade das informações de cunho pessoal que estão armazenadas no dispositivo informático.

O delito ora em comento consuma-se independente de algum resultado auferido à vítima, já que o simples ato de invadir furtivamente um dispositivo eletrônico, como aparelho celular, constitui o crime do Art. 154A. Logo, se pode dizer que recebe a característica de ser um delito formal.

O legislador preocupou-se em definir um aumento da pena para o delinquente caso este gere um prejuízo econômico para a vítima ou também divulgue o conteúdo daquilo que conseguiu obter de maneira clandestina.

Objetivando proteger determinadas pessoas que exercem cargos de extrema relevância no país, como Presidente da República e do Supremo Tribunal Federal, por exemplo, restaram estabelecidas penas mínimas e máximas maiores do que aquelas elencadas no caput do artigo, ou seja, uma forma qualificada do delito.

Diante da nova lei acrescida no cenário jurídico pátrio, a invasão de dispositivo que antes era conduta atípica deixou de ser considerado um ato preparatório para algum outro crime e agora é propriamente um delito previsto no Código Penal brasileiro.

2.3.2. Dano Informático

O dano informático pode também ser definido como sabotagem informática. Nesta infração penal o autor exerce o *animus nocendi* (desejo de destruir) para de forma consciente destruir, inutilizar ou deteriorar coisa alheia móvel, neste caso, poderia ser um site de uma empresa, um programa de computador ou até dados que constam armazenados em um dispositivo.

Juridicamente analisando, não se vislumbra um tipo penal especifico para abordar a conduta daquele que destrói dados informáticos. Sendo assim, necessário buscar dentro do ordenamento jurídico brasileiro, tipo penal que seja possível adequar determinado ato criminoso. Posto isto, dentro do Código Penal, o ilícito que mais se aproxima de certa ação seria o delito de Dano, previsto no Art. 163[43], conforme previsto abaixo:

> Art. 163 - Destruir, inutilizar ou deteriorar coisa alheia:
> Pena - detenção, de um a seis meses, ou multa.
> Dano qualificado
> Parágrafo único - Se o crime é cometido:
> I - com violência à pessoa ou grave ameaça;
> II - com emprego de substância inflamável ou explosiva, se o fato não constitui crime mais grave
> III - contra o patrimônio da União, de Estado, do Distrito Federal, de Município ou de autarquia, fundação pública, empresa pública, sociedade de economia mista ou empresa concessionária de serviços públicos;
> IV - por motivo egoístico ou com prejuízo considerável para a vítima:
> Pena - detenção, de seis meses a três anos, e multa, além da pena correspondente à violência.

Na concepção de Zaniolo[44] sabotagem informática é:

> "... todo e qualquer dano produzido, de modo intencional e sem permissão, em sistemas informatizados. Pode ser praticada por simples disseminação de códigos maliciosos em rede de computadores até a realização de severos ataques."

Crespo[45] demonstra ser possível a aplicação do Art. 163 para danos informáticos, somente:

---

[43] **CÓDIGO PENAL BRASILEIRO**, https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm, acesso em 16/12/2022.

[44] ZANIOLO, Pedro Augusto. **Crimes Modernos**: o impacto da tecnologia no direito. Salvador: Juspodium, 2021.

> "... com a destruição ou danificação da mídia que os arquiva (CDs-Rom, disquetes, pen drives, hard disks, memórias em geral) ou com o uso da informática. Por óbvio, havendo a destruição ou danificação de coisa material que contenha nela arquivados dados informáticos, aplicar-se-ia o art.163..."

O posicionamento do autor previsto no parágrafo anterior denota uma interpretação restritiva sobre o tema, deixando clarividente como é difícil tipificar os crimes modernos como os digitais praticados pela internet, mais precisamente, os crimes cibernéticos próprios.

Por outro lado, fazendo um contraponto a isto, é possível abordar a sabotagem informática dentro do Art. 202[46] do Código Penal, assim previsto:

> **Invasão de estabelecimento industrial, comercial ou agrícola. Sabotagem**
> Art. 202 - Invadir ou ocupar estabelecimento industrial, comercial ou agrícola, com o intuito de impedir ou embaraçar o curso normal do trabalho, ou com o mesmo fim danificar o estabelecimento ou as coisas nele existentes ou delas dispor:
> Pena - reclusão, de um a três anos, e multa.

Uma checagem mais minuciosa na segunda parte do artigo supra, vislumbra-se a ação de danificar o estabelecimento ou coisas nele existentes. Com o advento e crescimento do e-comerce houve uma proliferação de lojas virtuais que vendem seus diversos produtos por intermédio da internet.

Na mesma linha de entendimento, Zaniolo[47] destaca:

> "É notório que nos dias atuais os negócios e grande parte da economia se realizam e se desenvolvem através de negociações via web, por meio da rede mundial de computadores. Nesse sentido, o tradicional conceito de estabelecimento deverá, também, englobar aqueles que existem apenas na forma eletrônica, como alguns sítios de comércio eletrônico ou de prestação de serviços. (...) Portanto, a conduta de danificar o estabelecimento, que consiste em inutilizá-lo, parcial ou totalmente, por meio de ataque ao sítio onde se encontra hospedado, poderia configurar a prática do crime de sabotagem (informática)."

---

[45] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011.
[46] **CÓDIGO PENAL BRASILEIRO**, https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm, acesso em 16/12/2022.
[47] ZANIOLO, Pedro Augusto. **Crimes Modernos**: o impacto da tecnologia no direito. Salvador: Juspodium, 2021.

Portanto, sob esse prisma, destaca-se que as referidas lojas virtuais são estabelecimentos que possuem páginas na web que disponibilizam seu material para os consumidores. Então, todo e qualquer dano provocado contra as páginas destes estabelecimentos virtuais, constituem uma forma de sabotagem cometida pela web que encontra adequação perfeita ao disposto penal posto no artigo 202 do Codex.

2.3.3. Interceptação clandestina de dados informáticos e telemáticos

No tempo presente onde o computador e o smartphone assumiram o papel de pertencimento na vida de todas as pessoas no mundo, sendo usados como ferramentas de trabalho, de uso pessoal e no lazer, passando praticamente todo o tempo ao lado dos seus usuários.

Devido a isto ambos instrumentos passaram a armazenar dados pessoais e profissionais de extrema relevância, ao ponto de tornarem-se objetos essenciais e de grande valor.

Em busca desses dados (acesso a contas bancárias, segredos profissionais, cadastros pessoais) que criminosos criaram programas capazes de interceptar informações que transitam nesses aparelhos para na posse delas conseguir ganhos, principalmente, patrimoniais.

A interceptação de dados telemáticos e informáticos de maneira sorrateira, constitui delito previsto na lei de interceptações telefônicas, 9626/96. Na medida em que criminosos virtuais conseguem acesso em tempo real daquilo que é conversado através de aplicativos ou nas trocas de mensagens por e-mails sem a devida autorização judicial prévia, violam não só a legislação brasileira, como ofendem princípios constitucionais da privacidade e intimidade.

De acordo com a lei 9296/96, no seu art. 10[48], constituirá crime a ação daquele que interceptar comunicações telemáticas ou informáticas sem a autorização judicial ou com objetivos não autorizados em lei, senão vejamos:

[48] **Lei de Interceptação Telefônica**, 9296/1996. https://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em 03 de Janeiro de 2023.

> "Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, promover escuta ambiental ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei:
>
> Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa
>
> Parágrafo único. Incorre na mesma pena a autoridade judicial que determina a execução de conduta prevista no **caput** deste artigo com objetivo não autorizado em lei"

Na prática os crackers utilizam programas maliciosos que são inseridos de forma clandestina nos computadores ou telefones inteligentes. A partir dos acessos não autorizados o programa consegue captar todos os diálogos trocados por mensagens de e-mails ou por aplicativos e ao mesmo tempo disponibilizam para o delinquente digital.

Na cartilha[49] de segurança da internet é possível conceber melhor uma definição para esses programas, conhecidos como spyware que "é uma classe de programa de computador especialmente projetado para fins de monitoramento das atividades de um sistema, coletá-las e enviá-las a terceiros".

Em tese, é necessário o uso da rede mundial de computadores como meio para cometimento do crime, ao qual o atacante faz uso de alguma engenharia social, na maioria das vezes, para conseguir introduzir o programa malicioso, denominado de spyware, no dispositivo eletrônico da vítima e assim monitorar todos os passos dela.

2.3.4. Instalação de vírus e malwares com o cunho de se obter vantagem ilícita

O vírus é um programa malicioso que é introduzido em um sistema com o condão de destruir informações ou o próprio sistema, podendo ser replicado para outros equipamentos.

---

[49] CARTILHA de segurança da internet. **Comitê Gestor da Internet no Brasil**, jun. 2012. Disponível em: https://cartilha.cert.br/lvro/cartilha-seguranca-internet.pdf>. Acesso em: 03 de Janeiro de 2023.

Na visão de Ulbrich e Valle[50] a melhor definição de vírus seria:

> ".. são programas que se comportam como seus homônimos biológicos: são microscópicos, reproduzem-se sozinhos, consomem recursos computacionais que não lhes pertencem e têm alta capacidade de infecção por contágio. [...] Um vírus de computador possui objetivos muito claros: infectar o máximo possível de sistemas, reproduzir-se rapidamente e opcionalmente consumir recursos e danificar os sistemas invadidos.

Os diferentes tipos de vírus são destacados na Cartilha[51] de segurança da internet, entre os mais comuns estão:

> "... os programados por mensagens de correio eletrônico (e-mail), os vírus de script (executam determinadas funções, de acordo com a programação realizada pelo script), vírus de smartphone e os vírus de macro."

Com o decorrer do tempo, delinquentes digitais criaram uma variedade de vírus e com multifuncionalidades para atingir os equipamentos eletrônicos de usuários. Por isso, o vírus passou a ser uma espécie do gênero malware, como disserta Zaniolo[52]:

> "... Malware ou código malicioso é o termo geral utilizado para descrever os diferentes tipos de softwares usados com o objetivo de executar ações danosas e nos computadores, mas que também podem coletar informações pessoais (como as senhas dos usuários). Exemplos: vírus, spyware, ransomware, cavalos de troia (trojans) e worms."

Diante da diversidade de nomenclaturas que identificam o malware, alguns são bastante difundidos como os worms (vírus que se propagam usando as redes de comunicação e utilizam a própria rede de contatos dos usuários para fazer o autoenvio de e-mails e conseguir contaminar diversos computadores sem o auxílio humano). Também tem uma alta incidência o ransomware e os trojans (cavalos de tróia), o primeiro, o software infecta o sistema do computador da vítima e para permitir que funcione novamente os criminosos exigem uma quantia em dinheiro

---

[50] ULBRICH, Henrique César; VALLE, James Della. **Universidade H4CK3R**. 6 ED. São Paulo: Digerati Books, 2009.

[51] CARTILHA de segurança da internet. **Comitê Gestor da Internet no Brasil**, jun. 2012. Disponível em: https://cartilha.cert.br/lvro/cartilha-seguranca-internet.pdf>. Acesso em: 03 de Janeiro de 2023.

[52] Zaniolo, Pedro Augusto. **Crimes Modernos**: o impacto da tecnologia no direito. Salvador: Juspodium, 2021

(modalidade utilizada para atingir os computadores de grandes corporações e provocar vultuosos prejuízos), já o segundo, cavalo de tróia, seria um programa malicioso que é enviado pelo criminoso virtual para controlar todo o sistema de um computador.

De certa forma, todas as espécies de malwares causam visam algum tipo de vantagem ilícita e constitui crime previsto no Art.154A[53], segunda parte, do Código Penal, como é possível verificar a seguir:

> "Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou **de instalar vulnerabilidades para obter vantagem ilícita**:
>
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
>
> [...]"

Enfim, a função de instalar vulnerabilidades para obter vantagem ilícita, ou seja, a introdução de vírus ou outro tipo de malware é um crime virtual próprio já com previsão no Código Penal, impedindo que a sua propagação dentro do ambiente cibernético deixe de gerar consequências jurídicas, como algumas outras condutas que carecem de previsão e necessitam de uma interpretação extensiva. Diferente desta ação criminosa que tem na sua punição o seu principal desestímulo para os criminosos da internet.

2.4. Os tipos de cybercrimes impróprios de maior incidência no cenário brasileiro

Dentro do direito pátrio há uma variedade de delitos postos em legislações especiais e, na sua maioria, na estrutura do Código Penal. Na medida em que a sociedade evolui, os criminosos procuram variar na sua forma de utilizar o fator surpresa para atingir novas vítimas. É nessa ótica que surgem os crimes de internet impróprios, pois nada mais é que os crimes comuns cometidos através na rede mundial de computadores.

---

[53] **CÓDIGO PENAL BRASILEIRO**, https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm, acesso em 16/12/2022.

Barreto[54], estabelece como impuros ou impróprios:

> "...aqueles onde o dispositivo tecnológico é utilizado como meio para a prática do delito, propiciando a sua execução ou o seu resultado. Aqui apenas o veículo em que o crime é praticado é que envolve a tecnologia, sendo perfeitamente adequados diversas figuras típicas previstas no Código Penal Brasileiro ou em leis penais especiais."

O uso desse instrumento por quase toda totalidade do globo, leva o infrator a buscar adaptações aos atos considerados como típicos e o meio para práticas delitivas antigas somente ganhou nova roupagem, contudo continua atingindo os mesmos bens jurídicos atrelados ao indivíduo.

Didaticamente para melhor compreensão, Crespo[55] leciona:

> "... os crimes digitais impróprios nada mais são que aqueles já tradicionalmente tipificados no ordenamento, mas agora praticados com o auxílio de modernas tecnologias. Assim, essa denominação apenas representa que os ilícitos penais tradicionais podem ser cometidos por meio de novos *modus operandi*. Ocorre que alguns desses ilícitos ganham impressionante repercussão justamente por serem praticados por meio de ações envolvendo os meios tecnológicos."

Nos tópicos seguintes, serão ilustrados os crimes digitais impróprios mais corriqueiros nos dias atuais, analisando como eles têm dominado o cenário do registro de ocorrências dentro de uma delegacia de polícia.

2.4.1. Crimes contra a Vida.

Os crimes classificados como ofensivos ao bem jurídico vida se iniciam a partir do artigo 121 do CP e abrangem somente 4 tipos penais(homicídio, aborto, infanticídio e auxilio, induzimento e instigação ao suicídio), aos quais serão processados no âmbito do Tribunal do Júri e julgados por um conselho de sentença composto por 7 jurados, mais conhecido como Tribunal leigo.

Dentre os 04 delitos que compõem a estrutura da classificação de crimes que protegem a vida, o auxílio, induzimento e instigação ao Suicídio tem ganhado

---

[54]BARRETO, Alessandro Gonçalves/Brasil, Beatriz Silveira. **Investigação Cibernética,** à luz do Marco Civil da Internet. Rio de janeiro. Brasport, 2016.
[55]CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011.

corpo entre os mais jovens e a internet tem sido uma forma de disseminação desse crime.

2.4.1.1. Auxílio, Induzimento e Instigação ao Suicídio.

No bojo do Código Penal, mais precisamente, no artigo 122, há previsão de punição com pena de 6 meses à 2 anos de reclusão para aqueles que induzem, instigam ou auxiliam alguém a praticar a automutilação ou ao suicídio.

Nota-se que dentro da descrita lei não existe punição para a pessoa que pretende retirar sua própria vida, bem mais valoroso do ser humano, ou no caso da auto lesão, contudo não há permissão para que alguém incentive ou de alguma forma auxilie para que isso aconteça.

Pode-se observar, *in verbis*, no art. 122[56] do Código Penal, que o legislador acresceu causa majorante no dobro da pena, caso o delito previsto seja cometido em rede de computadores, senão vejamos:

> Art. 122. Induzir ou instigar alguém a suicidar-se ou a praticar automutilação ou prestar-lhe auxílio material para que o faça:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos
> § 1º Se da automutilação ou da tentativa de suicídio resulta lesão corporal de natureza grave ou gravíssima, nos termos dos §§ 1º e 2º do art. 129 deste Código:
> Pena - reclusão, de 1 (um) a 3 (três) anos.
> § 2º Se o suicídio se consuma ou se da automutilação resulta morte
> Pena - reclusão, de 2 (dois) a 6 (seis) anos.
> § 3º A pena é duplicada:
> I - se o crime é praticado por motivo egoístico, torpe ou fútil
> II - se a vítima é menor ou tem diminuída, por qualquer causa, a capacidade de resistência.
> § 4º A pena é aumentada até o dobro se a conduta é realizada por meio da rede de computadores, de rede social ou transmitida em tempo real
> § 5º Aumenta-se a pena em metade se o agente é líder ou coordenador de grupo ou de rede virtual.
> § 6º Se o crime de que trata o § 1º deste artigo resulta em lesão corporal de natureza gravíssima e é cometido contra menor de 14 (quatorze) anos ou contra quem, por enfermidade ou deficiência mental, não tem o necessário discernimento para a prática do ato, ou que, por qualquer outra causa, não pode oferecer resistência,

[56] **CÓDIGO PENAL BRASILEIRO**, https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm, acesso em 03/08/2022.

> responde o agente pelo crime descrito no § 2º do art. 129 deste Código.
> § 7º Se o crime de que trata o § 2º deste artigo é cometido contra menor de 14 (quatorze) anos ou contra quem não tem o necessário discernimento para a prática do ato, ou que, por qualquer outra causa, não pode oferecer resistência, responde o agente pelo crime de homicídio, nos termos do art. 121 deste Código.

A lei 13968 de 2019 trouxe nova redação ao caput do artigo e ainda incluiu novos parágrafos ora trazendo algumas causas de aumento de pena em alguns pontos, ora a qualificando em outros aspectos caso ocorra algum resultado ou envolva certa espécie de vítima.

Visando classificar o crime em comento, Cosenzo[57] enfatiza:

> "... a consumação do delito ocorre com a morte da vítima ou com a produção de lesão corporal de natureza grave. (...) Por similitude ao suicídio, a proteção visada é a integridade física, e na sequência, a vida humana, posta em risco com as reiterações de lesões corporais."

No escopo de destrinchar as três ações elencadas no tipo penal, Crespo[58] assevera que será punido:

> "... quem ajuda, instiga (reforça a ideia) ou induz (dá a ideia) outra a pessoa a se matar responde por crime. Assim, importa responsabilidade penal participar em suicídio de alguém seja de forma moral ou material, isto é, com palavras, gestos ou mesmo emprestando ferramentas para que a pessoa tire sua própria vida. O auxílio deve ser eficaz e contra pessoa determinada."

Conforme explanado em citação anterior, a vítima deve ser determinada e a ajuda exercida pelo criminoso deve ser eficaz, gerando algum tipo de resultado. Ocorre que na eventualidade dos atos de instigação, indução ou auxílio serem direcionados a pessoa com idade inferior a 14 anos ou caso ela não possua discernimento para prática do ato, ou seja, pessoas no catálogo de vulneráveis, haverá modificação do delito em comento para crime mais grave (homicídio), essa nova condição é extraída do parágrafo 7º do Art. 122.

---

[57] SILVA FILHO, Acácio Miranda da ... [et al.]; coordenadores Mauricio Schaun Jalil, Vicente Greco Filho. **Código Penal comentado**: doutrina e jurisprudência. Barueri [SP]: Manole, 2020.
[58] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011.

Lamentavelmente, muitos jovens são afetados pela cogitação da possibilidade de suicídio, em algumas situações existem comunidades, vídeos tutoriais na internet e até desafios que venham a desencadear pessoas a retirar a própria vida.

Por isso, o crime de auxílio, induzimento e instigação ao suicídio passou a figurar como mais uma modalidade de crimes de internet. Nessa linha de pensamento, os autores Furlaneto Neto, Santos e Gimenes[59] exemplificam:

> "No caso da internet, esta constitui mais uma forma de se praticar o delito do Art. 122, e isso pode ocorrer em especial nas duas primeiras modalidades, ou seja, induzir e instigar que de forma direta em conversas de salas de bate-papo ou de redes sociais, quer por meio de sites específicos que ensinam como cometer suicídio."

O crescimento desse tipo de infração penal praticado na web cresceu de maneira tão assustadora que o legislador, em 2019, resolveu inserir uma majorante para o delito do Art. 122 no dobro da pena, se a conduta for realizada por meio de rede de computadores, de rede social ou transmitida em tempo real. Nesse mister, Consenzo[60] evidencia:

> "No sentido de prevenir e retribuir a conduta do agente por meio de rede de computadores, de rede social ou transmitida em tempo real, a pena será aumentada até o dobro. A pena também será aumentada em metade se o agente for líder ou coordenador de grupo ou rede virtual."

Na tentativa de ilustrar possibilidades usadas pelos infratores que adotam a internet como ambiente para atuar, Zaniolo[61] denota:

> "Em salas virtuais de bate papo, candidatos ao suicídio trocam informações acerca dos melhores locais e das formas mais céleres (e também menos dolorosas) de suprimir a própria vida. Na maioria desses casos, as pessoas só se conhecem pessoalmente na hora do encontro para morrer, mantendo contato anterior somente por meio de mensagens eletrônicas."

O mesmo autor Zaniolo[62] continua destacando:

---

[59]FURLANETO NETO, Mário; SANTOS, José Eduardo Lourenço dos; GIMENES, Eron Veríssimo. **Crimes na internet e inquérito policial eletrônico**. São Paulo: Edipro, 2012.

[60] SILVA FILHO, Acácio Miranda da ... [et al.]; coordenadores Mauricio Schaun Jalil, Vicente Greco Filho. **Código Penal comentado**: doutrina e jurisprudência. Barueri [SP]: Manole, 2020.

[61] ZANIOLO, Pedro Augusto. **Crimes Modernos**: o impacto da tecnologia no direito. Salvador: Juspodium, 2021.

[62] ZANIOLO, Pedro Augusto. **Crimes Modernos**: o impacto da tecnologia no direito. Salvador: Juspodium, 2021.

> "Os parágrafos 4º e 5º, incluídos pela sobredita Lei 13.968/2019, preveem a conduta deste crime cometido pela internet. No §4º o exemplo clássico é o Whatsapp. Por meio de conversações pode-se induzir alguém a se suicidar."

Sobre a mesma temática, Masson[63] cita um dos casos bastante disseminados entre os jovens que constitui crime cibernético previsto no at.122, assim preleciona:

> "Destaca-se o ritual da Baleia Azul (Blue Whale Challenge), surgido na Rússia em 2013, cujos participantes eram submetidos aos integrantes automutilações, que iam se agravando ao avançarem-se as fases, cujo desafio final era o suicídio."

Implicando na mesma toada, arrolando mais algumas casuísticas de ocorrência do delito estudado, Crespo[64] discorre:

> "Pessoas que criem comunidades em redes sociais com dicas e fóruns de como tirar a própria vida ou, ainda, que relacionando-se com outras empregam termos como, o mundo seria melhor sem você fulano, se mate, cometem o crime."

Diante de diversas situações aqui citadas pelos autores, é perceptível casos clássicos e, outros mais atuais, de formas de cometimento do crime de auxílio, instigação e induzimento ao suicídio por intermédio da rede mundial de computadores. A preocupação é tamanha que levou o legislador, em 2019, a promover uma alteração no código penal e findar por inserir causas de aumento para criminosos que optem utilizar a rede virtual como meio de prática delitiva.

2.4.2. Crimes contra a Honra

Os crimes que tutelam a honra encontra-se no bojo do Código Penal, mais precisamente no seu capítulo 5. Nele há a distribuição de três modalidades de infração penal: a calúnia, difamação e injúria, aos quais protegem as honras objetiva e subjetiva da pessoa.

O primeiro dos delitos está elencado no Art. 138[65] do CP recebendo a denominação de Calúnia cuja definição mais adequada seria caluniar alguém,

---

[63] MASSON, Cleber**. Direito Penal**: parte especial (arts. 121 a 212). São Paulo: Método, 2020.
[64] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011.
[65] **CÓDIGO PENAL BRASILEIRO**, https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm, acesso em 03/08/2022.

atribuindo a terceiro fato falso que constitui crime. Logo, o crime em destaque visa defender a honra objetiva de terceiro, assim elencado:

> 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.

Na lição dos autores Gamil Hireche e Gabriel de Oliveira[66] a objetividade jurídica do crime previsto no art. 138, seria:

> "O bem jurídico tutelado no delito de calúnia é, portanto, a honra. A calúnia atinge a honra em seu aspecto objetivo, uma vez que traduz desprestígio à boa fama de que goza o sujeito perante seu grupo social."

Sem dúvidas o crime de calúnia e demais contra a honra, são perfeitamente amoldados aos delitos virtuais impróprios, a título exemplificativo Crespo[67] menciona como possível crime quando em "um chat, espalhar e-mails ou publicar em redes sociais que determinada pessoa abusou sexualmente de outra ou que desviou quantias em dinheiro da empresa".

Seguindo a linha de pensamento similar, a Difamação[68], art. 139 do CP, consiste na imputação de fato ofensiva à reputação de outrem. Segundo os autores Gamil Hireche e Gabriel de Oliveira[69] o fato "deve ser ofensivo à reputação. Isto é, deve repercutir na boa fama de que goza a vítima no âmbito de seu grupo social".

> Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação:
>
> Pena - detenção, de três meses a um ano, e multa.
>
> **Exceção da verdade**

---

[66] SILVA FILHO, Acácio Miranda da ... [et al.]; coordenadores Mauricio Schaun Jalil, Vicente Greco Filho. **Código Penal comentado**: doutrina e jurisprudência. Barueri [SP]: Manole, 2020.
[67] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011.
[68] **CÓDIGO PENAL BRASILEIRO**, https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm, acesso em 03/08/2022.
[69] SILVA FILHO, Acácio Miranda da ... [et al.]; coordenadores Mauricio Schaun Jalil, Vicente Greco Filho. **Código Penal comentado**: doutrina e jurisprudência. Barueri [SP]: Manole, 2020.

> Parágrafo único - A exceção da verdade somente se admite se o ofendido é funcionário público e a ofensa é relativa ao exercício de suas funções.

Já a Injúria[70], previsto no Art. 140 do CP, seria a conduta de injuriar alguém como forma de denegrir a sua dignidade atingindo a honrar subjetiva. Nele estão os xingamentos que atingem diretamente a pessoa, porém nada impede do seu cometimento através da internet. Para Noronha[71] (1973, P.123) "o bem jurídico tutelado é a honra em sua esfera subjetiva, a estima própria, o juízo que a pessoa faz de si mesma, a sua dignidade ou decoro".

> Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:
> Pena - detenção, de um a seis meses, ou multa.
> § 1º - O juiz pode deixar de aplicar a pena:
> I - quando o ofendido, de forma reprovável, provocou diretamente a injúria;
> II - no caso de retorsão imediata, que consista em outra injúria.
> § 2º - Se a injúria consiste em violência ou vias de fato, que, por sua natureza ou pelo meio empregado, se considerem aviltantes:
> Pena - detenção, de três meses a um ano, e multa, além da pena correspondente à violência.
> § 3o Se a injúria consiste na utilização de elementos referentes a raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência:
> Pena - reclusão de um a três anos e multa.

É possível destacar no §3º do artigo acima transcrito, que o legislador atribui a chamada injúria discriminatória aos atos ofensivos a raça, cor, religião, origem, condição de pessoa idosa ou portadora de deficiência, prevendo uma pena ainda maior quando comparada com ela elencada no caput do art. 140.

De forma clara e direta, Crespo[72] enumera como situações de difamação e injúria como crimes digitais:

> "... de difamação: em ambiente de rede social ou espalhando e-mails alguém diz que é comum ver determinada pessoa drogando-se ou prostituindo-se. (...) de injúria: em ambiente de redes sociais ou mediante envio de e-mail descrevem-se e comentam-se características negativas de uma pessoa, chamando-a de gorda, vaca, imbecil etc".

---

[70] **CÓDIGO PENAL BRASILEIRO**, https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm, acesso em 05/08/2022.
[71] NORONHA, Magalhães. **Direito Penal**: crimes contra a pessoa e crimes contra o patrimônio. São Paulo, 1973.
[72] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011.

Concebendo como possível estabelecer para todos os delitos contra a honra a qualidade de ser também cometidos por autores dentro do ambiente virtual, Furlaneto Neto[73] afirma que:

> "...são compatíveis com suas práticas por meio de internet, a qual, nos casos citados, funciona apenas como um novo *modus operandi* para que se possa ter a ofensa da honra, quer na sua forma objetiva, quer na forma subjetiva. Com isso percebe-se que nenhuma alteração legislativa é necessária ocorrer para a tipificação da calúnia, difamação ou injúria praticadas por meio da rede mundial de computadores".

O crescente uso do ambiente virtual para cometimento dos crimes contra a honra, local onde os usuários acreditam não haver normas de condutas e não ser alcançados pelo código penal, levou o legislador em 2019 a inserir novas causas de aumento de pena para todos os delitos dessa natureza. Destarte, foi colocado no corpo do art. 141[74], no seu parágrafo §2º, na parte das disposições comuns, aumento de pena, como podemos ver a seguir:

> Art. 141 - As penas cominadas neste Capítulo aumentam-se de um terço, se qualquer dos crimes é cometido:
> I - contra o Presidente da República, ou contra chefe de governo estrangeiro;
> II - contra funcionário público, em razão de suas funções, ou contra os Presidentes do Senado Federal, da Câmara dos Deputados ou do Supremo Tribunal Federal;
> III - na presença de várias pessoas, ou por meio que facilite a divulgação da calúnia, da difamação ou da injúria.
> IV - contra criança, adolescente, pessoa maior de 60 (sessenta) anos ou pessoa com deficiência, exceto na hipótese prevista no § 3º do art. 140 deste Código
> § 1º - Se o crime é cometido mediante paga ou promessa de recompensa, aplica-se a pena em dobro
> **§ 2º Se o crime é cometido ou divulgado em quaisquer modalidades das redes sociais da rede mundial de computadores, aplica-se em triplo a pena. (grifo nosso)**

Logo, os delitos contra a honra cometidos ou divulgados através das redes sociais da rede mundial de computadores terá sua pena aumentada no triplo. Assim, nítida demonstração de que tais ações merecem atenção e punição exemplar como forma de inibir a propagação desarrazoada dessa modalidade delituosa.

---

[73] FURLANETO NETO, Mário; SANTOS, José Eduardo Lourenço dos; GIMENES, Eron Veríssimo. **Crimes na internet e inquérito policial eletrônico**. São Paulo: Edipro, 2012.

[74] **CÓDIGO PENAL BRASILEIRO**, https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm, acesso em 05/08/2022.

2.4.3. Ameaça

Na seara dos crimes contra a liberdade individual é previsto a Ameaça, definido como o intuito de ameaçar alguém por palavras, gestos ou qualquer outro meio visando um mal injusto e grave.

Apesar de ser um crime de menor potencial ofensivo, encontra-se no rol dos mais frequentes no contexto dos registros nas delegacias de polícia. Da mesma forma, atualmente, está entre os delitos virtuais mais cometidos, pois infratores usam rede social ou aplicativos, como whatsapp, para desejar um mal injusto e grave a outrem.

Alcazar[75] explica que no mencionado delito

> "O núcleo do tipo é o verbo ameaçar, que significa intimidar, atemorizar, prometer castigo ou malefício. (...) Poderá a ameaça ser direta(refere-se a pessoa ou patrimônio da vítima) ou indireta (a promessa refere-se a terceira pessoa ligada à vítima), explícita (manifesta de forma induvidosa), implícita (formulada de forma velada) e ainda condicional (o mal prometido está na dependência de um acontecimento futuro).

A objetividade jurídica do crime estudado, segundo Alcazar[76] é "a liberdade individual psíquica da pessoa humana, sua tranquilidade, sua paz de espírito. Protege-se a livre manifestação da vontade, que é tolhida pela ameaça".

Os autores Furlano Neto, Santos e Gimenes[77] descrevem que "a internet veio a se apresentar, assim como ocorreu com os crimes contra a honra, como sendo mais um meio, um mecanismo, um instrumento (modus operandi) para ameaçar alguém".

Já Crespo[78] atribui como exemplo da ameaça virtual, "enviar e-mails ou publicar em redes sociais dizeres como 'vou te pegar', 'pode reservar uma vaga no cemitério' ".

---

[75] SILVA FILHO, Acácio Miranda da ... [et al.]; coordenadores Mauricio Schaun Jalil, Vicente Greco Filho. **Código Penal comentado**: doutrina e jurisprudência. Barueri [SP]: Manole, (2020, P.432).
[76] SILVA FILHO, Acácio Miranda da ... [et al.]; coordenadores Mauricio Schaun Jalil, Vicente Greco Filho. **Código Penal comentado**: doutrina e jurisprudência. Barueri [SP]: Manole, (2020, P.432).
[77] FURLANETO NETO, Mário; SANTOS, José Eduardo Lourenço dos; GIMENES, Eron Veríssimo. **Crimes na internet e inquérito policial eletrônico**. São Paulo: Edipro, (2012, P. 42).
[78] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, (2011, P.88).

Mencionando situações hipotéticas sobre esse crime na sua forma virtual, Zaniolo[79] denota que comete a ameaça aquele que “envia mensagens eletrônicas à vítima, prometendo difamá-la gravemente em redes sociais e, ainda, sugerindo males indeterminados que poderiam acometer sua família”.

De mais a mais, a diversidade de formas dessa prática criminosa tem ganhado destaque pela crescente de registros formais quando se faz o uso de meio virtual. O desconhecimento dos limites da rede mundial de computadores conjuntamente com a enganosa sensação de impunidade, permite uma propagação da ameaça virtual em diferentes contextos, como salas de bate papo, aplicativos e páginas na web. É relevante a intervenção do legislador criando uma exasperação de pena para essa nova forma de ação e de alguma forma servir de prevenção para conscientizar os que ainda insistem em infringir a lei e desrespeitar o direito do próximo.

2.4.4. Crimes Contra o Patrimônio

Diante de um gama de delitos que protegem o patrimônio alguns foram criados na modalidade específica como uma forma muito própria de crimes digitais, entre eles o furto e o estelionato classificados como eletrônicos. A importância dada pelo legislador pátrio para ambos os crimes ocorreu devido a uma crescente de ações que passaram a atingir uma quantidade expressiva de vítimas e, na mesma proporção, por uma lacuna legislativa, as diversas condutas criminosas deixavam de ser punidas. Logo, dois fatores foram preponderantes para um olhar mais atento do congresso nacional brasileiro, o aumento de pessoas lesadas por essas modalidades delitivas e o aumento da impunidade.

Pelo motivo exposto, findou como necessária a adequação da legislação e uma inserção de novos dispositivos no código penal, para evitar que a sensação de impunidade se propagasse por todo o seio da sociedade e deixassem a nova categoria de criminosos, cyber criminosos, alheios à legislação brasileira.

---

[79] ZANIOLO, Pedro Augusto. **Crimes Modernos**: impacto da tecnologia no direito. Salvador: Juspodium, (2021, P. 238).

2.4.4.1. Furto Eletrônico

O delito de Furto vem disposto no artigo 155[80] do Código Penal, e prevê como conduta punitiva ação daquele que subtrai coisa alheia móvel de outra pessoa, em suma, é a subtração do patrimônio de forma não violenta.

> **Art. 155 - Subtrair, para si ou para outrem, coisa alheia móvel:**
>
> Pena - reclusão, de um a quatro anos, e multa.
>
> § 1º - A pena aumenta-se de um terço, se o crime é praticado durante o repouso noturno.
>
> § 2º - Se o criminoso é primário, e é de pequeno valor a coisa furtada, o juiz pode substituir a pena de reclusão pela de detenção, diminuí-la de um a dois terços, ou aplicar somente a pena de multa.
>
> § 3º - Equipara-se à coisa móvel a energia elétrica ou qualquer outra que tenha valor econômico.
>
> **Furto qualificado**
>
> § 4º - A pena é de reclusão de dois a oito anos, e multa, se o crime é cometido:
>
> I - com destruição ou rompimento de obstáculo à subtração da coisa;
>
> II - com abuso de confiança, ou mediante fraude, escalada ou destreza;
>
> III - com emprego de chave falsa;
>
> IV - mediante concurso de duas ou mais pessoas.
>
> § 4º-A A pena é de reclusão de 4 (quatro) a 10 (dez) anos e multa, se houver emprego de explosivo ou de artefato análogo que cause perigo comum. (Incluído pela Lei nº 13.654, de 2018)
>
> § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo. (Incluído pela Lei nº 14.155, de 2021) (Grifo nosso)
>
> § 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso: (Incluído pela Lei nº 14.155, de 2021)
>
> I – aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional; (Incluído pela Lei nº 14.155, de 2021)

[80] **CÓDIGO PENAL BRASILEIRO**, https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm, acesso em 03/08/2022.

> II – aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável. (Incluído pela Lei nº 14.155, de 2021)
>
> § 5º - A pena é de reclusão de três a oito anos, se a subtração for de veículo automotor que venha a ser transportado para outro Estado ou para o exterior. (Incluído pela Lei nº 9.426, de 1996)
>
> § 6o A pena é de reclusão de 2 (dois) a 5 (cinco) anos se a subtração for de semovente domesticável de produção, ainda que abatido ou dividido em partes no local da subtração. (Incluído pela Lei nº 13.330, de 2016)
>
> § 7º A pena é de reclusão de 4 (quatro) a 10 (dez) anos e multa, se a subtração for de substâncias explosivas ou de acessórios que, conjunta ou isoladamente, possibilitem sua fabricação, montagem ou emprego. (Incluído pela Lei nº 13.654, de 2018)

Destrinchando melhor tal delito que protege o patrimônio, Grecco[81] disserta:

> "Percebe-se, portanto, que o mencionado tipo penal é composto por vários elementos, a saber: o núcleo subtrair; o especial fim de agir caracterizado pela expressão para si ou para outrem; bem como pelo objeto da subtração, ou seja, a coisa alheia móvel. O verbo subtrair é empregado no artigo *sub examen* no sentido de retirar, tomar, sacar do poder de alguém coisa alheia móvel. A finalidade de ter a coisa alheia móvel para si ou para outrem é que caracteriza o chamado *animus furandi* do delito de furto."

A crescente subtração de dinheiro em contas e subtração de dados pessoais e informações bancárias advindas de e-mails maliciosos ou por intermédio de aplicativos de troca de mensagens evidenciou uma nova modalidade de furto. Nesse sentido, em 2021, foi promulgada a lei 14.155 que acresceu ao código penal, dentro do artigo 155, qualificadora de pena de 4 a 8 anos caso o furto fosse cometido por fraude utilizando dispositivo eletrônico ou informático.

Pretendendo melhor esclarecimento dessa modalidade de furto mediante fraude Estefan[82] sustenta:

> **"**Quando, porém, o furto mediante fraude ocorrer com a utilização de dispositivo eletrônico ou informático, se caracterizará a figura especial do § 4º-B. Assim, *v.g.*, quando o sujeito obtém a senha bancária e os dados de *login* da vítima e realiza transferência

[81] GRECCO, Rogério. **Curso de Direito Penal**: parte especial, volume III. Niterói: Impetus, (2015, P.6).
[82] ESTEFAN, André. **Direito Penal**: Parte Especial – Arts. 121 a 234-C – v. 2. São Paulo : SaraivaJur, (2022, P.714).

> bancária não autorizada, subtraindo os valores correspondentes da conta corrente do ofendido".

Ainda sob o mesmo prisma, continua Estefan[83] diferenciando dispositivo eletrônico de dispositivo informático, ao qual:

> Entende-se por **dispositivo informático** o mecanismo físico ou virtual capaz de reunir informações ou dados digitalizados em ambiente eletrônico, por meio da linguagem característica dos computadores e mecanismos equivalentes. São exemplos: PC (*personal computer*), *tablet*, *smartphone*, *flashdrive* ou p*endrive.* Segundo Spencer Sydow, trata-se de "qualquer *hardware* que trabalhe com o trato automático de informações e possua em si capacidade de armazenamento de dados confidenciais. Já o **dispositivo eletrônico**, por exclusão, compreende o aparato eletrônico que não trabalhe com informações ou dados digitalizados. De ver que, com o avanço da tecnologia, praticamente todos os dispositivos eletrônicos contêm, ainda que de forma rudimentar, algum *hardware* que trabalhe com informações e armazenamento de dados. Pode-se citar como exemplo desta figura a subtração realizada pelo agente que, valendo-se de seu *smartphone*, acessa a conta bancária da vítima e, sem que ela saiba, furta quantia em dinheiro ali depositada, transferindo-a para outra conta corrente.

O legislador foi ainda mais além no escopo de reduzir drasticamente a quantidade de condutas que ficavam fora de previsão dentro da lei, passando a admitir qualquer outro meio análogo à fraude eletrônico, dando uma interpretação ampla para o que se considera furto eletrônico. Assim sendo, Greco[84] leciona que:

> **"**Qualquer outro meio fraudulento análogo à fraude cometida por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso também importará na aplicação da qualificadora. (...) Uma vez instalados, os códigos maliciosos passam a ter acesso aos dados armazenados no computador e podem executar ações em nome dos usuários, de acordo com as permissões de cada usuário. Os principais motivos que levam um atacante a desenvolver e a propagar códigos maliciosos são a obtenção de vantagens financeiras, a coleta de informações confidenciais, o desejo de autopromoção e o vandalismo. Além disso, os códigos maliciosos são, muitas vezes, usados como intermediários e possibilitam a prática de golpes, a realização de ataques e a disseminação de *spam*."

---

[83] ESTEFAN, André. **Direito Penal**: Parte Especial – Arts. 121 a 234-C – v. 2. São Paulo : SaraivaJur, (2022, P.714).
[84] GRECO, Rogério. **Curso de direito penal**: volume 2: parte especial : artigos 121 a 212 do código penal. Barueri [SP] : Atlas, (2022, P. 1227).

2.4.4.2. Extorsão

Na esfera de tutela ao patrimônio, é previsto no artigo 158[85] do CP o crime de Extorsão que como simples definição é a ação de obrigar alguém a fazer, deixar de fazer ou tolerar que seja feito certo ato que configure uma vantagem econômica para o criminoso que sempre agirá com violência ou grave ameaça.

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

Greco[86] tecendo algumas considerações sobre o delito em estudo afirma:

> "... deve atuar com uma finalidade especial, que transcende ao seu dolo, chamada de especial fim de agir, aqui entendida como o intuito de obter para si ou para outrem indevida vantagem econômica. Dessa forma, o agente deve constranger a vítima, impondo-lhe um comportamento – positivo ou negativo -, determinando que faça, tolere que se faça, ou mesmo deixe de fazer alguma coisa, a fim de que, com isso, consiga, para ele ou para outrem, indevida vantagem econômica, que deve ser entendida em um sentido mais amplo do que a coisa móvel alheia, ou seja, passível ou não de remoção, poderá se constituir na finalidade especial com que atua o agente."

A utilização em massa das redes sociais e de aplicativos de troca de texto, fotos e vídeos, como o whatsapp e telegram, chamou a atenção dos

---

[85] **CÓDIGO PENAL BRASILEIRO**, https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm, acesso em 08/08/2022.

[86] GRECCO, Rogério. **Curso de Direito Penal**: parte especial, volume III. Niterói: Impetus, (2015, P.96).

criminosos virtuais para identificar vítimas em potencial e novas formas de conseguir dinheiro. Desta forma, multiplicou-se a extorsão como delito cibernético impróprio. Atualmente, os meliantes conseguem fotografias em redes sociais ou no perfil de aplicativos, em seguida, entram em contanto pelo chat do instagram ou facebook, ou mesmo, pelo número que consta o whatsapp, e simula fazer parte de uma famosa facção criminosa que atual em diversos estados do Brasil. Ato contínuo ameaça a pessoa de morte e solicita que faça transações bancárias para uma conta informada pele autor.

O *modus operandi* aqui narrado, infelizmente tem se tornado corriqueiro e atinge pessoas de diferentes classes sociais, seja de baixa instrução escolar e, até mesmo, com alta instrução escolar, podendo assim dizer que não há uma vítima em potencial, mas sim uma escolha aleatória.

Buscando ilustrar nova forma de execução da extorsão, Zaniolo[87] cita que "um cidadão condenado pelo crime de extorsão teria utilizado imagens de uma mulher, com quem se relacionava virtualmente, para conseguir dinheiro em troca de não divulgação do material pornográfico".

Na mesma toada, válido exemplificar duas situações de extorsão virtual, muito comuns, a primeiro já narrada pelo autor Zaniolo no parágrafo anterior, que é de pessoas que conseguem fotos de vítimas em situações como sem roupa ou fazendo sexo e depois ameaçam colocar em rede social e enviar para familiares, caso não seja transferido uma quantia em dinheiro. Já a segunda, afeta grandes corporações, aos quais crackers conseguem acessar o sistema dessas empresas e subtrair muitas informações importantes, em seguida solicitam pagamento de valores em troca de não destruição daquelas informações relevantes.

A primeira forma de subespécie de extorsão abordada é conhecida como sextorsão. Nesta conduta o autor consegue as fotos os vídeos íntimos da vítima, seja invadindo o dispositivo ou pela entrega espontânea da pessoa, ato contínuo a obriga a mandar mais fotos e vídeos, ou mesmo a enviar uma quantia em dinheiro como forma de não tornar público aquele material.

---

[87] Zaniolo, Pedro Augusto. **Crimes Modernos**: o impacto da tecnologia no direito. Salvador: Juspodium, (2021, P.372).

2.4.4.3. Estelionato Eletrônico

Dando continuidade aos delitos contra o patrimônio que são usualmente mais utilizados pelos criminosos virtuais, encontra-se o Estelionato, disposto no Art. 171[88] do CP, que representa a punição para aquele criminoso que visa obter para si vantagem ilegal provocando prejuízo na vítima através do uso de algum artifício, conversa ardilosa ou algum outro método fraudulento.

> 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.
> (...)
>
> **Fraude eletrônica**
>
> **§ 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo. (Incluído pela Lei nº 14.155, de 2021) (Grifo nosso)**
> **§ 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional. (Incluído pela Lei nº 14.155, de 2021) (Grifo nosso)**
> **§ 3º - A pena aumenta-se de um terço, se o crime é cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência.**
>
> Estelionato contra idoso ou vulnerável (Redação dada pela Lei nº 14.155, de 2021)
> § 4º A pena aumenta-se de 1/3 (um terço) ao dobro, se o crime é cometido contra idoso ou vulnerável, considerada a relevância do resultado gravoso. (Redação dada pela Lei nº 14.155, de 2021)
> § 5º Somente se procede mediante representação, salvo se a vítima for:
> I - a Administração Pública, direta ou indireta;
> II - criança ou adolescente;
> III - pessoa com deficiência mental; ou
> IV - maior de 70 (setenta) anos de idade ou incapaz.

---

[88] **CÓDIGO PENAL BRASILEIRO**, https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm, acesso em 08/08/2022.

Para melhor compreender a definição de delito em discussão, Greco[89], contudo leciona:

> "Sendo a fraude o ponto central do delito de estelionato, podemos identifica-lo, outrossim, por meio dos seguintes elementos que integram a sua figura típica: a) conduta do agente dirigida finalisticamente à obtenção de vantagem ilícita em prejuízo alheio; b) a vantagem ilícita pode ser para o próprio agente ou para terceiro; c) a vítima é induzida ou mantida em erro; d) o agente se vale de um artifício, ardil, ou qualquer meio fraudulento para a consecução do seu fim."

O mesmo autor Greco[90] completa o raciocínio afirmando:

> "O crime de estelionato é regido pelo binômio vantagem ilícita/prejuízo alheio. A conduta do agente, portanto, deve ser dirigida a obter vantagem ilícita, em prejuízo alheio. (...) a vítima sofre prejuízo, também, de natureza econômica. Assim, poderá perder aquilo que já possuía, a exemplo daquele que entrega determinada quantia ao estelionatário, ou mesmo deixar de ganhar o que lhe era devido (...) a utilização da fraude pelo agente visa induzir ou manter a vítima em erro. Erro significa a concepção equivocada da realidade, é um conhecimento falso do que ocorre no mundo real. (...) Induzir a erro é fazer nascer a representação equivocada na vítima. O agente, mediante sua fraude, cria no espírito da vítima um sentimento que não condiz com a realidade."

A lacuna na legislação nacional para abarcar as variadas fraudes advindas de chats, redes sociais (facebook e instagram) e aplicativos (whatsapp e telegram) que utilizam a internet, mobilizou o congresso nacional em prol de uma mudança, principalmente dentro do Código Penal.

Perante essa realidade, em 2021, foi aprovado projeto de lei 14.155 prevendo a nova modalidade de estelionato conhecido como estelionato eletrônico, cujo promoveu o aumento da pena de reclusão de 4 a 8 anos.

De acordo com o que pode ser extraído do parágrafo §2º A do Art. 171, considera-se estelionato eletrônico toda a fraude que usa informações de vítimas

---

[89]GRECCO, Rogério. **Curso de Direito Penal**: parte especial, volume III. Niterói: Impetus, (2015, P.237).
[90]GRECCO, Rogério. **Curso de Direito Penal**: parte especial, volume III. Niterói: Impetus, (2015, P.237).

que são levadas a erro através de redes sociais, contato telefônico ou envio de correio eletrônico fraudulento.

No intuito de enumerar situações do novo tipo de estelionato, Estefan[91] cita:

> "... como exemplo, o sujeito que envia diversos *e-mails* a endereços aleatórios que obtém facilmente na própria internet e, na mensagem, oferece alguma promoção ou vantagem, mas a condiciona ao fornecimento de informações pessoais mediante preenchimento de um cadastro *online*, utilizando-se, posteriormente, de tais dados para praticar golpes. Ou, ainda, o agente que realiza contato telefônico com o ofendido e simula ser funcionário de algum órgão governamental coletando informações para uma pesquisa ou dados para vacinação, posteriormente fazendo uso do que lhe foi revelado pela vítima ludibriada para obtenção de vantagem indevida. Outro caso corrente é o golpe do WhatsApp, em que o sujeito convence o ofendido, mediante ardil, a lhe passar os dados e o controle do aplicativo e, depois de obter o controle, age como se fosse a vítima e manda mensagens a seus contatos pedindo dinheiro "emprestado". Serão sujeitos passivos do estelionato qualificado todos os que tiverem prejuízo em razão do golpe praticado."

Pretendendo demonstrar situações corriqueiras de estelionato eletrônico, Furlano Neto, Santos e Gimenes[92] ilustram:

> "... o sujeito ativo cria um site de comércio eletrônico para a venda de produtos informáticos, ofertando os produtos a preços convidativos e prometendo a entrega em 15 dias úteis, mediante o pagamento em depósito do valor em conta corrente. Nesse período, contabiliza o lucro com as vendas fraudulentas, sem fazer nenhuma entrega, de forma que, após um tempo, retira o site do ar, deixando inúmeras vítimas em prejuízo. Outra hipótese que pode vir a caracterizar o estelionato é a venda de bens em sites hospedeiros, como, por exemplo, um par de tênis, em que o suposto vendedor oferece o produto que pode ser adquirido por outrem mediante lance, de forma que, após a vítima ser declarada vencedora, o agente exige o pagamento em conta corrente para fazer a entrega do bem, porém

[91] ESTEFAN, André. **Direito Penal**: Parte Especial – Arts. 121 a 234-C – v. 2. São Paulo : SaraivaJur, (2022, P.873).
[92] FURLANETO NETO, Mário; SANTOS, José Eduardo Lourenço dos; GIMENES, Eron Veríssimo. **Crimes na internet e inquérito policial eletrônico**. São Paulo: Edipro, (2012, P. 65)

> ao invés do tênis oferecido, o agente envia à vítima, via sedex, uma pedra."

A fim de trazer a baila, situações comuns de fraudes eletrônicas utilizadas por criminosos virtuais, Cunha[93]:

> "**a) por meio de redes sociais:** atualmente são muito comuns os anúncios promovidos em redes sociais como Facebook e Instagram. Não raro, são anúncios fraudulentos, manobras ardilosas para atrair pessoas que forneçam seus dados; (...) **c) pelo envio de correio eletrônico fraudulento:** neste caso, a vítima recebe um e-mail fraudulento, muitas vezes imitando os caracteres de empresas ou organizações conhecidas e, a partir do acesso por meio do *link* disponibilizado, o estelionatário pode obter os dados pessoais e bancários inseridos em formulários eletrônicos; **d) por qualquer outro meio fraudulento análogo:** nesta fórmula analógica se inserem quaisquer outras práticas fraudulentas cometidas por meios eletrônicos ou informáticos, como páginas na *internet*, por exemplo, em que a vítima não é diretamente abordada pelo estelionatário, como nas modalidades anteriores, mas é induzida em erro por fatores diversos (simulação de um estabelecimento comercial regularmente constituído; cópia de outra página conceituada etc.)."

A variedade de fraudes registradas nas ocorrências das delegacias de polícia de todo o Brasil, demonstram duas coisas: a primeira que o estelionato eletrônico já supera as demais formas convencionais de estelionato, no segundo ponto deixam nítidas que os criminosos estão preferindo atuar no ambiente virtual devido a facilidade da sua transnacionalidade e extraterritorialidade, assim como pela dificuldade de identificação dos infratores.

2.4.5. Incitação e Apologia ao Crime

Na busca da proteção da paz pública estão os delitos de incitação e apologia ao crime. Ambas tipologias criminais conseguem perfeitamente se amoldar aos delitos virtuais impróprios.

A incitação ao crime tem a sua ocorrência com a incitação pública a algum delito, havendo previsão no código penal no artigo 286[94], in verbis:

---

[93] CUNHA, Rogério Sanches. **Lei 14.155/21 e os crimes de fraude digital. Primeiras impressões e reflexos no CP e no CPP**. In https://meusitejuridico.editorajuspodivm.com.br/2021/05/28/lei-14-15521-e-os-crimesdefraude-digital-primeiras-impressoes-e-reflexos-no-cp-e-no-cpp/.(2021) Acessado 18 de 0utubro de 2022.

> Art. 286 - Incitar, publicamente, a prática de crime:
>
> Pena - detenção, de três a seis meses, ou multa.
>
> Parágrafo único. Incorre na mesma pena quem incita, publicamente, animosidade entre as Forças Armadas, ou delas contra os poderes constitucionais, as instituições civis ou a sociedade.

O delito em estudo para ser de fato considerado infração penal precisa ser direcionado a um número indeterminado de pessoas e em ambiente público, pois se for direcionado a somente uma pessoa ou a incitação ocorrer em ambiente privado, não haverá ocorrência delitiva.

Nessa linha de pensamento, Alexandre Patara[95] denota:

> "A vontade de incitar alguém à prática de um crime deve ser clara e específica. O tipo penal em análise contém, em sua descrição, a necessidade de o fato deve ser público (...) essa elementar normativa do tipo, publicidade do ato, é indispensável para a consecução da prática do ato, pois somente atingindo o maior número de pessoas possível é que caracteriza a ofensa a paz pública."

O ambiente virtual tornou-se um campo perfeito e recorrente para que usuários incitem a violência contra um grupo de pessoas devido a sua opção sexual, opinião política ou identidade racial. A propagação desse crime é feito em salas de bate papo virtual, via twiter, comunidades em redes sociais e até na criação de páginas na rede.

Noutro giro, o elogio, enaltecimento ou exaltação a um crime passado ou mesmo à figura de um criminoso caracteriza a figura penal da Apologia ao Crime. A mencionada conduta criminosa figura no Art. 287[96] do Código Penal e evidencia que a apologia deve ser feita publicamente.

> Art. 287 - Fazer, publicamente, apologia de fato criminoso ou de autor de crime:
>
> Pena - detenção, de três a seis meses, ou multa.

---

[94] **CÓDIGO PENAL BRASILEIRO**, https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm, acesso em 10/08/2022.

[95] SILVA FILHO, Acácio Miranda da ... [et al.]; coordenadores Mauricio Schaun Jalil, Vicente Greco Filho. **Código Penal comentado**: doutrina e jurisprudência. Barueri [SP]: Manole, (2020, P.741).

[96] **CÓDIGO PENAL BRASILEIRO**, https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm, acesso em 10/08/2022.

Na visão de Alexandre Patara[97] o delito de apologia ao crime tem como melhor definição:

> "O ato de exaltar um criminoso ou uma prática criminosa, feito publicamente além de moralmente reprovável. (...) A conduta descrita no tipo penal e estudo consiste em fazer apologia publicamente de fato criminoso ou de autor de crime. Apologia significa exaltar, elogiar, enaltecer, louvar, aprovar, defender, destacar. (...) A exaltação, nesse caso, faz referência a crimes e fatos delituosos."

Na mesma toada, Fragoso[98] assevera que a apologia seria "o elogio e a exaltação do malefício ou do mal feitor, em que constituem estímulo e sugestão às vontades débeis e as pessoas propensas ao crime".

A consumação do crime de apologia depende da sua publicidade e a internet é o local perfeito e bastante utilizado nos dias atuais para isso. Comumente, na rede mundial de computadores, é visto o enaltecimento às práticas nazistas e outras formas de genocídio cometidas em diferentes partes do mundo buscando destacar também a figura dos genocidas.

Cassanti[99] destaca que os criminosos estão "usando os sites de relacionamento para propagar fotos com armas, vídeos enaltecendo o crime e incentivando o uso de drogas, fazendo clara apologia a diversos crimes e facções criminosas".

Visando ilustrar situações que configurariam os crimes de apologia e incitação ao crime, Crespo[100] evidencia:

> "... aqueles que aderem a certas comunidades e grupos de discussão na internet podem vir a responder por tais ilícitos. Portanto quem fizer parte de comunidades destinadas a veicular o preconceito mediante agressões a outras pessoas e o consumo ou tráfico de drogas pode vir a ser responsabilizado por este crime".

Sem sombra de dúvidas, tanto o delito de Apologia ao crime como o de incitação ao criminoso ou à prática criminosa são cometidos na sua grande maioria

---

[97] SILVA FILHO, Acácio Miranda da ... [et al.]; coordenadores Mauricio Schaun Jalil, Vicente Greco Filho. **Código Penal comentado**: doutrina e jurisprudência. Barueri [SP]: Manole, (2020, P.742/743).
[98] FRAGOSO. Henleno Cláudio. **Lições de direito penal**: Parte Especial. 11ed. Atualiz. Por Fernando Fragoso. Rio de Janeiro: Forense, (2005, P.277).
[99] CASSANTI, Moisés de Oliveira. **Crimes Virtuais**, **vítimas reais.** Rio de Janeiro: Brasport, (2014, P. 33).
[100] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, (2011, P.88).

por usuários da internet. Na proporção que aumenta as pessoas conectadas, cresce também essas espécies delitivas, uma vez que é um vasto campo onde as pessoas usam para manifestar sua opinião e defender seus pontos de vista sobre uma variedade de temas.

2.4.6. Falsa Identidade

De acordo com a vasta doutrina, a falsa identidade é o crime atribuído àquela pessoa que se identifica como se outra pessoa fosse, ou mesmo, confere a terceiro identificação que não seria a verdadeira, sempre com o intuito de prejudicar alguém ou obter algum tipo de vantagem.

Além da definição acima descrita, também é considerado falsa identidade quando alguém utiliza como próprio algum documento de terceiro, como o passaporte, título de eleitor, carteira de habilitação ou de identidade. Do mesmo modo, responderá por esse delito a pessoa que cede documento de terceiro para uso indevido.

As duas modalidades de falsa identidade narradas nos parágrafos anteriores, podem ser melhor delineadas nos artigos 307[101] e 308[102] do Código Penal, como se pode observar *in verbis*:

> Art. 307 - Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem:
>
> Pena - detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave.
>
> Art. 308 - Usar, como próprio, passaporte, título de eleitor, caderneta de reservista ou qualquer documento de identidade alheia ou ceder a outrem, para que dele se utilize, documento dessa natureza, próprio ou de terceiro:
>
> Pena - detenção, de quatro meses a dois anos, e multa, se o fato não constitui elemento de crime mais grave.

---

[101] **CÓDIGO PENAL BRASILEIRO**, https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm, acesso em 12/08/2022.

[102] **CÓDIGO PENAL BRASILEIRO**, https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm, acesso em 12/08/2022

Didaticamente para melhor compreensão, Greco[103] leciona:

> O delito de *falsa identidade* veio tipificado no art. 307 do Código Penal. De acordo com a redação típica, podemos apontar os seguintes elementos: *a)* a conduta de atribuir-se falsa identidade; *b)* a atribuição de falsa identidade a terceiro; *c)* a finalidade de obter vantagem, em proveito próprio ou alheio; *d)* ou de causar dano a outrem. *Ab initio*, o núcleo *atribuir* é utilizado pelo texto legal no sentido de imputar. Assim, o agente imputa a si mesmo, ou a terceira pessoa, falsa identidade. Por *identidade* devemos entender o conjunto de caracteres próprios de uma pessoa, que permite identificá-la e distingui-la das demais, a exemplo do nome, idade, profissão, sexo, estado civil etc. A lei pune a autoatribuição falsa, ou a atribuição falsa a terceiro, isto é, o agente se identifica incorretamente, com dados que não lhe são próprios, ou atua, da mesma forma, atribuindo esses dados falsos a terceira pessoa.

Embora o infrator se intitule alguém que não seja, é preciso prejudicar alguém ou obter algum tipo de vantagem, para a consumação delitiva. Afastando as vantagens sexuais e econômicas, por que podem figurar diferentes tipos penais como violação sexual mediante fraude e, respectivamente, estelionato, Hungria[104] esclarece que o proveito:

> "...pode ser de ordem moral ou representar qualquer outra utilidade não econômica (ex.: pelo prazer de favorecer a um amigo, o agente atribui-se a respectiva identidade para, em lugar dele, prestar um exame num concurso), assim como a vantagem colimada pode não depender necessariamente do prejuízo alheio ou este não estar em reciprocidade com vantagem alguma."

Adentrando na seara dos delitos virtuais, Zaniolo[105] ilustra algumas situações de como o crime em estudo é utilizado pelos cyber criminosos. Dessa forma, descreve:

> "Além do correio eletrônico, também é possível a conduta delituosa em comento utilizando-se de ferramentas como aplicativos de mensagens instantâneas (whatsapp e Facebook Messenger), redes sociais, sítios web, etc., onde os internautas se fazem passar por outras pessoas para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem. A criação de perfis falsos (ou fakes) nas redes sociais também configura este crime. Inclusive, tal prática de utilizar identidade falsa para fins fraudulentos na Internet (conhecida como sockpuppet, algo como fantoche) para fins da conduta de catfishing, buscando-se obter vantagem, em proveito

---

[103] GRECO, Rogério. **Curso de direito penal**: volume 2: parte especial : artigos 121 a 212 do código penal. Barueri [SP] : Atlas, (2022, P. 1484/1485).
[104] HUNGRIA, Nélson. **Comentários ao código penal**. São Paulo: Forense, (2007, P.308).
[105] ZANIOLO, Pedro Augusto. **Crimes Modernos**: o impacto da tecnologia no direito. Salvador: Juspodium, (2021, P. 242/243).

> próprio ou alheio, ou para causar dano a outrem em romances fraudulentos.

No mesmo contexto, no escopo de discorrer também situações de falsa identidade cometida em ambiente virtual, Crespo[106] exemplifica:

> "...celebridades e famosos em geral usam a internet e as redes sociais cada vez mais. Isso também faz crescer os perfis falsos, conhecidos por "fakes", que são pessoas que se passam por outras. (...) uma pessoa se faz passar por quem não é, utilizando dados e até mesmo senha de outra pessoa, em proveito próprio ou alheio, ou para causar dano a outrem."

Pensando sobre um viés mais prático, dificilmente, quando a matéria é crime digital, há cometimento da falsa identidade sem alguma associação com outro delito de diferente espécie. Hoje, criminosos atribuem à sua pessoa outra identidade e cria um perfil falso para ludibriar diferentes vítimas e praticar o estelionato, ou cria perfis falsos em redes sociais para denegrir a honra de outrem, ou mesmo, fazer apologia e incitação a vários crimes. Assim como, exercem a identidade de terceiros para acessar sistema de bancos e subtrair dinheiro, ou atrair vítimas para cometer crimes sexuais.

De certa forma, como exposto, é possível notar que o delito de Falsa Identidade pode ser usado perfeitamente como meio para a consumação de outro crime cibernético, demonstrando que o legislador ainda não percebeu o seu grau de importância dentro da seara dos novos delitos, carecendo de uma tipificação mais específica e com maior punição, como fez nos crimes contra a honra, no furto e no estelionato.

2.4.7. Crimes contra a Dignidade Sexual

2.4.7.1. Estupro Virtual

No estupro a liberdade sexual é deixada de lado pelo infrator e fazendo ele do uso da grave ameaça ou da violência pratica atos sexuais libidinosos ou conjunção carnal, contra a vontade da vítima.

---

[106] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, (2011, P. 88/89).

No bojo do Código Penal, elencado no Art. 213[107], encontra-se o delito de estupro, senão vejamos:

> Art. 213. Constranger alguém, mediante violência ou grave ameaça, a ter conjunção carnal ou a praticar ou permitir que com ele se pratique outro ato libidinoso
>
> Pena - reclusão, de 6 (seis) a 10 (dez) anos
>
> § 1o Se da conduta resulta lesão corporal de natureza grave ou se a vítima é menor de 18 (dezoito) ou maior de 14 (catorze) anos
>
> Pena - reclusão, de 8 (oito) a 12 (doze) anos
>
> § 2o Se da conduta resulta morte:
>
> Pena - reclusão, de 12 (doze) a 30 (trinta) anos.

De forma bastante clara, Estefan[108] leciona as duas formas de conduta que envolvem o crime de estupro, assim, na sua visão:

> "Há duas formas de cometer o estupro: praticar o ato (o que supõe participação mais ativa da vítima) e permitir que se pratique (que sugere atitude passiva do ofendido, o qual é obrigado a suportar a conduta do agente). Não é necessário que haja contato físico entre o autor do constrangimento e a vítima. O agente pode, por exemplo, obrigá-la a se masturbar diante dele, sem tocá-la em momento algum."

Como destacado, no crime em discussão não se exige o contato físico entre a vítima e o autor, consumando perfeitamente nas situações em que o autor mediante ameaça obriga a vítima a masturbar-se ou introduzir certos objetos nas suas partes íntimas, violando sua liberdade sexual e satisfazendo a lascívia do criminoso.

Dentro dessa seara de não contato físico que surge o estupro virtual. Na medida em que cresce o contato das pessoas por rede social, os criminosos aproveitam-se disso para aproximar-se das vítimas e contra elas cometer todo e qualquer tipo de crime, inclusive de cunho sexual.

---

[107] **CÓDIGO PENAL BRASILEIRO**, https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm, acesso em 12/10/2022.

[108] ESTEFAN, André. **Direito Penal**: Parte Especial – Arts. 121 a 234-C – v. 2. São Paulo : SaraivaJur, 2022, p.1065.

Nessa mesma linha, Greco[109] demonstra e exemplifica situações possíveis do crime cibernético denominado de estupro virtual, conforme seu entendimento:

> "Poderá ocorrer, inclusive, a hipótese do chamado *estupro virtual*, ou à *distância*, em que, por exemplo, o agente, por meio de uma webcam, ou mesmo através de programas de telefones celulares, nos quais se pode efetuar chamadas de vídeo, tal como ocorre com o WhatsApp, constrange a vítima, mediante grave ameaça, a praticar, nela própria, atos libidinosos, forçando-a a se masturbar. Verifica-se, portanto, a falta de necessidade de contato físico do agente, que poderá estar a milhares de quilômetros de distância do seu agressor, restando, da mesma forma, configurado o estupro."

Corroborando este raciocínio, Barros[110] afirma ser "plenamente possível virtualmente alguém ser constrangido, mediante violência ou grave ameaça a praticar ou permitir que com ele se pratique atos libidinosos ou até mesmo conjunção carnal".

Certamente, uma abordagem extremamente nova, porém cada vez mais comum, na medida em que infratores virtuais na posse informações valiosas sobre certas pessoas usam da grave ameaça para exigir da vítima a automasturbação, como exemplo, cometendo assim o estupro virtual, modalidade de delito digital contra a liberdade sexual.

Após discorrer sobre os diferentes crimes cibernéticos próprios e impróprios existentes e cometidos no Brasil, necessário se faz apresentar quais medidas jurídicas encontradas no ordenamento jurídico pátrio que possam ser utilizadas na proteção dos bens jurídicos vinculados aos seres humanos.

2.5. Do Arcabouço legislativo no ordenamento jurídico brasileiro como base para proteção de direitos e o combate aos delitos digitais

Uma rápida passagem pela história da internet no capítulo sobre a Era Digital é facilmente perceptível como o Brasil viveu um vácuo legislativo quando a matéria é a proteção de direitos da personalidade dentro do ambiente virtual.

---

[109] GRECO, Rogério. **Curso de direito penal**: volume 3: parte especial : artigos 213 a 361 do código penal. Barueri [SP] : Atlas, 2022, p. 281.
[110] BARROS, Francisco Dirceu. **Tratado doutrinário de direito penal**. Salvador: Juspodium, 2018, p. 1.540.

Tanto é que somente em 2022 foram feitas algumas alterações na Constituição Federal elevando os direitos pessoais nos meios digitais como direito fundamental. Também nessa mesma ótica foi incorporada no ordenamento jurídico brasileiro a Lei Geral de Proteção de Dados Pessoais no ano de 2018, tutelando inclusive os dados pessoais no âmbito digital.

Um pouco mais anterior, já no ano de 2012, foi promulgada a Lei 12.737/12 denominada de lei Carolina Dieckmann que introduziu no Código Penal Brasileiro os primeiros delitos cibernéticos propriamente ditos.

Não deixando de destacar ainda, leis que envolvam a matéria, vislumbra-se o Marco Civil da Internet no ano de 2014 e o mais antigo destes institutos que é a lei de Interceptação Telefônica, Informática e Telemática promulgada no ano 1996.

Além dos acima citados, o Código Penal Brasileiro, já modificado em diversas oportunidades, inclusive algumas das suas mudanças foram inseridas novas tipificações penais, dentre elas o acréscimo de crimes virtuais, entre o rol de delitos previstos no mencionado Código.

O propósito do presente trabalho não é esgotar todos os instrumentos normativos que elencam alguma passagem sobre delitos virtuais. Destarte, necessário se faz tecer alguns comentários sobre os principais textos normativos dentro do ordenamento jurídico pátrio.

2.5.1. Emenda Constitucional nº 115/2022

A dinâmica social e o maciço uso dos meios tecnológicos e da internet pela população exigiram do legislador constituinte a elevação dos dados pessoais na esfera digital à direito fundamental.

Após o surgimento da Lei Geral de Proteção aos Dados Pessoais, carecia de um sustentáculo constitucional da proteção desses direitos o que se consolidou agora no ano de 2022.

Sendo assim, a Pec 17 de 2019, promoveu uma alteração no Art. 5º da CF, mais precisamente introduzindo o novo inciso 79. Segundo o novo texto da Carta Magna, o Art. 5º, inciso LXXIX[111] é previsto:

> **EMENDA CONSTITUCIONAL Nº 115, DE 10 DE FEVEREIRO DE 2022**
>
> Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.
>
> As Mesas da Câmara dos Deputados e do Senado Federal, nos termos do § 3º do art. 60 da Constituição Federal, promulgam a seguinte Emenda ao texto constitucional:
>
> Art. 1º O caput do art. 5º da Constituição Federal passa a vigorar acrescido do seguinte inciso LXXIX:
>
> "Art. 5º (...)
>
> LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais."

Como bem assevera Hermes Canhas[112], a proteção de dados anteriormente era alicerçada no direito fundamental à privacidade e proteção à vida privada. Segundo este autor:

> "...é uma afirmação clara de que a proteção de dados agora é tema a ser defendido, valorizando a LGPD, que agora tem direcionamento específico constitucional que a recepciona. EM linhas objetivas, a quem defenda que uma vez aprovada a PEC não há que si falar em entendimento doutrinário jurisprudencial em contrário.. E se antes a proteção de dados era derivada do gênero de direitos à intimidade e à proteção da vida privada, agora a proteção de dados será individualmente apontada como garantia fundamental."

---

[111] Constituição Federal Brasileira, http://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm, acesso em 16 de Setembro de 2022.

[112] CANHAS, Hermes. **Garantismo Constitucional quanto à Lei de Proteção de Dados (LGPD) e Pec 17/2019**: influências, impactos e desenvolvimento da Proteção de Dados. www.hermescanhas.jusbrasil.com.br. Acesso em 10 de Setembro de 2022.

Na mesma esteira, o autor Ingo Wolfgang Sarlet[113], ressalta que antes mesmo da emenda constitucional considerar a proteção de dados pessoais digitais à direito constitucionalmente resguardado, já era possível tutelar a sua proteção em outros direitos constitucionais expostos na Carta Magna Brasileira, senão vejamos

> "... na condição de direito fundamental explicitamente autônomo, no texto da CP, e a exemplo do que ocorreu em outras ordens constitucionais, o direito à proteção dos dados pessoais pode (e mesmo deve) ser associado e reconduzido – exatamente como fez o STF – a alguns princípios e direitos fundamentais de caráter geral e especial, como é o caso do princípio da dignidade da pessoa humana, do direito fundamental(também implicitamente positivado) ao livre desenvolvimento da personalidade, do direito geral de liberdade, bem como dos direitos especiais de personalidade mais relevantes no contexto, quais sejam – aqui nos termos da CF – os direitos à privacidade e à intimidade, e um direito à livre disposição sobre os dados pessoais, o assim designado direito à livre autodeterminação informativa."

Importante frisar que como direito fundamental a proteção dos dados pessoais por meios digitais possui eficácia imediata e foi elencada no Art. 5º da atual Constituição Federal. Em momento anterior possuía uma tutela implícita dentre outros direitos constitucionalmente firmados, diferente da tratativa dada atualmente. É de suma importância a atenção dada pelo legislador constituinte que demonstra acompanhar a dinâmica social e sua preocupação com a vulnerabilidade de pessoas da sociedade que na medida em que utilizam mais e mais a internet ficam expostos às ofensas aos seus direitos básicos.

2.5.2. Lei Geral de Proteção de Dados

No ano de 2018, foi promulgada a Lei Geral de Proteção de Dados Pessoais (LGPD), lei 13.709/18, visando proteger os direitos fundamentais de liberdade e de privacidade quando se refere ao contato com dados pessoais nos meios digitais por pessoas físicas ou jurídicas.

---

[113] SARLET, Ingo Wolfgang. **A EC115/22 e a proteção dos dados pessoais como Direito Fundamental**. www.conjur.com.br. Acesso em 12 de Setembro de 2022.

É possível observar o objetivo acima descrito já no Artigo 1º[114] da Lei 13.709/18, ao qual prevê:

> "Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural."

Ao falar sobre crimes digitais, difícil não apontar um delito que não afronte ou exponha os dados pessoais das vítimas, dados estes prescritos no ambiente virtual. Por isso, como forma de evitar a exposição desnecessária desses dados e sujeição deles à risco potencial, o legislador pátrio resolveu criar um regramento para proteger tais informações inerentes à pessoa.

Para melhor compreensão da tomada de decisão para criação da legislação específica na proteção de informações pessoais, Miragem[115], descreve como principal motivo:

> "...a decisão político-jurídica de diversos sistemas jurídicos no sentido de disciplinar a coleta e, sobretudo, o tratamento de dados pessoais por intermédio da legislação específica sobre o tema. O Brasil associou-se a este esforço de disciplina legislativa da proteção de dados pessoais com a edição, em 2018, da lei 13.709, de 14 de agosto de 2018 (LGL/2018/7222) denominada Lei Geral de Proteção de Dados (LGPD). Fundamenta-se a LGPD no propósito de garantia dos direitos do cidadão, oferecendo bases para o desenvolvimento econômico a partir da definição de marcos para a utilização econômica da informação decorrente dos dados pessoais."

Ainda sobre os objetivos da legislação em comento, Monteiro[116] delineia que:

> "... tem por objetivo não apenas conferir às pessoas mais controle sobre seus dados, mas também fomentar um ambiente de desenvolvimento econômico e tecnológico, mediante regras flexíveis e adequadas para lidar com os mais inovadores modelos de negócio baseados no uso de dados pessoais. (...) A LGPD também busca equilibrar interesses econômicos e sociais, garantindo a continuidade de decisões automatizadas e também limitando abusos nesse

---

[114] **LEI GERAL DE PROTEÇÃO DE DADOS**, lei 13.709/18, http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 01/10/2022.

[115] MIRAGEM, Bruno. **A Lei Geral de Proteção de Dados (Lei 13.704/2018) e o direito do Consumidor**. Revistas dos Tribunais. Vol. 1009/2019. Nov/2019, p. 02.

[116] MONTEIRO, Renato Leite. **Existe um direito à explicação na Lei Geral de Proteção de Dados no Brasil?** Instituto Igarapé. Artigo Estratégico nº 39. Dezembro de 2018.

> processo, por meio da diminuição de assimetria das informações, e, por consequências, de poder, entre o indivíduo, setor privado e o Estado."

Nesta esteira, claramente a lei ordinária explicita em seu corpo alguns fundamentos, como pode ser observado no Art. 2º[117] da Lei 13.704/18, in verbis

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Esclarecendo o primeiro fundamento da lei, Garcia[118] assevera:

> "Nesse 2º artigo da lei, o primeiro fundamento é a privacidade. É importante destacar que proteção de dados e privacidade são questões diferentes. Por exemplo, se uma pessoa publicar um dado em sua página pessoal numa rede social, ela se torna público. Entretanto, isso não significa que esse dado pode ser utilizado indiscriminadamente. Aquele que vier a utilizá-lo, deve respeitar os direitos do titular dos dados, previstos na LGPD. Tais dados, portanto, não estão sob a égide do princípio constitucional da privacidade, mas sim sob o escopo da proteção de dados."

Sobre o segundo fundamento da lei Garcia[119] continua em sua afirmação elencando que

> "O segundo fundamento é a autodeterminação informativa, cujo significado está em garantir que o titular tenha o direito de decidir o que será feito com a sua informação, em saber quais dados as Organizações possuem, como elas os utilizam e se ele quer que seu dado esteja com eles, quer seja utilizado ou não. Em outras palavras, de acordo com esse fundamento, cada pessoa natural determina como sua informação pode (e se vai) ser utilizada."

---

[117] MONTEIRO, Renato Leite. **Existe um direito à explicação na Lei Geral de Proteção de Dados no Brasil?** Instituto Igarapé. Artigo Estratégico nº 39. Dezembro de 2018

[118] GARCIA, Lara Rocha. **Lei Geral de Proteção de Dados Pessoais (LGPD):** Guia de implantação/ Lara Rocha Garcia; Edson Aguilera Fernandes; Rafael Augusto Moreno Gonçalves; Marcos Ribeiro Pereira-Barretto. São Paulo: Bluchen, 2020, p. 17.

[119] GARCIA, Lara Rocha. **Lei Geral de Proteção de Dados Pessoais (LGPD):** Guia de implantação/ Lara Rocha Garcia; Edson Aguilera Fernandes; Rafael Augusto Moreno Gonçalves; Marcos Ribeiro Pereira-Barretto. São Paulo: Bluchen, 2020, p. 17.

> Sob outro prisma, agora traçando considerações sobre a lei como importante marco normativo Mendes[120] denota a percepção:
> "que a LGPD foi um importante passo rumo ao fortalecimento do marco normativo da sociedade da informação no Brasil. É preciso agora desenvolver uma cultura de dados, construir uma sólida estrutura institucional para a aplicação da LGPD, propiciando segurança jurídica para os atores da economia digital, a proteção da confiança do titular dos dados e incentivando o desenvolvimento econômico do país nessa área."

Vale lembrar que o presente preceito legal pode ser visto como um "escudo" de proteção para as vítimas dos delitos cibernéticos quanto à invasão e exposição dos dados pessoais, entretanto ao mesmo tempo deve ser usado como base de sustentação dos pedidos administrativos e judiciais no escopo de instrumentalizar um inquérito policial.

2.5.3. Lei 12.965/2014 (Marco Civil da Internet)

Até o ano de 2014, comentar sobre internet era um conteúdo de conhecimento coletivo, porém sem regramento dentro do Brasil, situação que levava a um vasto campo de violações de direitos e total ausência de deveres por parte daqueles que a utilizavam. Daí a necessidade de amparo legal motivando a criação da lei 12.965 do ano de 2014, denominada de Marco Civil da Internet.

Para melhor compreensão sobre o objeto da legislação especial, Fiorillo[121] esclarece:

> "... o denominado Marco Civil da Internet (Lei 12.965/2014), ao pretender estabelecer princípios, garantias, direitos e deveres vinculados à manifestação do pensamento, à criação, à expressão e à informação (meio ambiente cultural), por meio do uso da internet no Brasil (meio ambiente digital) procura de qualquer forma tentar organizar parâmetros jurídicos específicos no âmbito infraconstitucional destinado a tutelar o conteúdo da comunicação social e mesmo dos direitos e deveres fundamentais da pessoa humana por meio do uso de computadores no Brasil em redes

---

[120] MENDES, Laura Schertel; DONEDA, Danilo**. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados**. Revista de Direito do Consumidor, São Paulo, v. 120, ano 27, p. 469- 483, nov./dez. 2018. Disponível em: https://revistadedireitodoconsumidor.emnuvens.com.br/rdc/article/view/1116. Acesso em: 10 jul. 2022.
[121] FIORILLO, Celso Antônio Pacheco. **O Marco Civil da Internet e o Meio Ambiente Virtual na Sociedade da Informação**: Comentários à Lei 12.965/2014, (2015, P.5/6).

> interligadas visando, ao que tudo indica, destacar a importância da tutela jurídica da internet no século XXI em nosso País."

No intuito de encontrar uma melhor definição para o Marco Civil da Internet que Barreto e Brasil[122] atribuem como "uma norma específica a regular as relações no ambiente virtual, trazendo em seu bojo os fundamentos da disciplina do uso da internet no Brasil". Deixando claro que agora o ambiente virtual passa a ter regras a serem seguidas e respeitadas, não sendo mais um local primitivo.

Teffé e Moraes[123] manifestam-se sobre de que forma a nova lei contribuiu para dar mais segurança aos usuários de mundial de computadores e, no entender deles, destaca-se:

> "... o acidentado, embora vitorioso, percurso do Marco Civil da Internet (MCI) que, em virtude de causar impactos diretos nos interesses empresariais e enfrentar uma série de temas que ainda estavam abertos – como a proteção aos registros, aos dados pessoais e às comunicações privadas; a neutralidade da rede, a responsabilidade civil dos provedores de conexão e das aplicações de internet, a guarda de dados e registros e a requisição judicial de registros, passou por um longo processo de debate legislativo, terminando com a sua aprovação em 23 de abril de 2014, tornando-se a lei 12.965"

Atualmente, o Marco Civil aparece como uma poderosa arma na proteção dos direitos pessoais digitais dos usuários e vítimas de crimes praticados no âmbito da internet. É possível, por exemplo, fazer requerimentos administrativos para provedores de internet e administradores de páginas da web e solicitar cadastros e retirada de conteúdo lesivo à bens jurídicos de indivíduos.

A título de exemplificação, da forma em que a dita lei pode ser usada como instrumento de combate aos abusos dentro do ambiente virtual, Barreto e Brasil[124] ilustram:

> " Quando alguém, por exemplo, promove insultos a outrem em rede social, ofendendo-o em razão de sua religião, ou, ainda, quando

---

[122] BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira. Manual **de Investigação Cibernética: à luz do Marco Civil da Internet.** Rio de Janeiro: Brasport, 2016, p. 10.

[123] TEFFÉ, Chiara Spadaccini de; MORAES, Maria Celina Bodin de. **Redes Sociais Virtuais**: privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet. Revistas de Ciências Jurídicas. V.22. Fortaleza: Pensar, 2017, p. 111.

[124] BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira. Manual **de Investigação Cibernética: à luz do Marco Civil da Internet.** Rio de Janeiro: Brasport, 2016, p. 11.

> revende na internet passagens aéreas compradas com cartões clonados, conseguindo comercializá-las a preços baixos bem abaixo do mercado, está atentando contra os fundamentos do Marco Civil da Internet, desvirtuando a função social da internet."

As situações aqui trazidas pelos autores explicitam como os diferentes delitos cometidos através das redes virtuais trazem prejuízos à pessoas físicas e jurídicas, afetando nitidamente o Marco Civil da Internet.

Ao fazer uma análise de como agiu o legislador na criação de um mecanismo defensivo e ao mesmo tempo atuante contra os abusos, Teffé e Moraes[125] concluem:

> "... entendeu o legislador que os intermediários, marcadamente os grandes e organizados provedores, têm a possibilidade e o dever de contribuir com a segurança dos usuários da rede, devendo retirar, conteúdos considerados lesivos, dentro de critérios razoáveis, quando instados a fazê-lo (...) o MCI estabelece como regra que o provedor de aplicações deverá retirar o conteúdo apontado como danoso, embora somente após ordem judicial específica. Entretanto, caso se trate de conteúdo que viole frontalmente a privacidade de uma pessoa – imagens, vídeos ou outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado – o provedor terá o dever de retirar o material em seguida ao recebimento da notificação extrajudicial enviada pela vítima."

Nesse espeque, Barreto e Brasil[126] asseveram como objetivo da lei especial:

> "A preocupação com os usuários da internet mais uma vez é manifestada no diploma legal, seja garantindo-lhe voz (expressão, comunicação, manifestação do pensamento e participação) na rede, seja protegendo-lhes a intimidade e a privacidade, ou, ainda, assegurando-lhes acesso seguro e de qualidade ao mundo digital"

Diante de algumas considerações, se pode concluir que o MCI surgiu como importante instrumento de balizamento do uso da internet, criando regras, garantindo direitos e impondo deveres aos usuários e provedores (pessoas jurídicas). A própria lei criou mecanismos administrativos de socorro à violação de

---

[125] TEFFÉ, Chiara Spadaccini de; MORAES, Maria Celina Bodin de. **Redes Sociais Virtuais**: privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet. Revistas de Ciências Jurídicas. V.22. Fortaleza: Pensar, 2017, p. 142.

[126] BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira. Manual **de Investigação Cibernética: à luz do Marco Civil da Internet.** Rio de Janeiro: Brasport, 2016, p. 11.

direitos, ao mesmo passo estabeleceu limites para liberdade dos provedores combatendo sua imparcialidade frente ao nítido desrespeito aos direitos individuais, ou seja, colocou o provedor também na posição de vigilante dos seus próprios usuários e o alçou a uma posição mais próxima do protagonismo.

De mais a mais essa lei especial foi um verdadeiro marco, como o próprio nome dado a ela, colocando um freio aos crimes ditos como digitais que eram cometidos irrestritamente e sem controle dentro da web. Hoje, tornou-se mais um escudo de proteção aos direitos fundamentais das pessoas e instrumento de uso de aplicadores da lei, principalmente, dos agentes atuantes na esfera da polícia judiciária.

2.5.4. A Lei 12.737/12 (Carolina Dieckmann) e o Decreto Lei 2848 de 1940 (Código Penal Brasileiro)

No ano de 2013, a lei ordinária 12.737 de 2012, denominada de Lei Carolina Dickmann, foi promulgada e inseriu crimes dentro do Código Penal, basicamente os artigos 154A e 154B, além disso, alterou os artigos 266 e 298 do mesmo Codex.

A citada lei, como bem explana Zaniolo[127] adquiriu essa nomenclatura em homenagem a uma atriz devido a:

> "... crackers (hacker maliciosos) do interior de Minas Gerais e São Paulo invadirem o computador da atriz Carolina Dieckmann, de onde copiaram as suas fotos íntimas. O conteúdo foi publicado na Internet após ela resistir às chantagens, no valor de 10 mil reais, para que as imagens fossem apagadas. O caso serviu de combustível para agilizar a aprovação da nova lei em 03.12.2012."

Interessante destacar que a dita norma representou um importante marco dentro do Código Penal Brasileiro, já que trouxe à baila a tipificação dos primeiros delitos virtuais. Algo extremamente novo para a realidade dos operadores do direito e uma nítida demonstração da iniciativa do legislador de acompanhar a dinâmica

[127] ZANIOLO, Pedro Augusto. **Crimes Modernos**: Os impactos da Tecnologia no Direito. Salvador: Editora JusPodium, 2021, p. 650.

social e introduzir no campo punitivo condutas atreladas a um novo momento vivido pela sociedade.

O Código Penal merece destaque, pois elenca em seu corpo a grande maioria dos delitos que têm em algumas das suas condutas o cometimento através da internet, crimes de informáticas impróprios, embora no presente momento também passe a prevê crimes cibernéticos propriamente ditos, como aqueles dos artigos 154A e 154B.

Uma vez raçados diplomas legais que exercem um cunho protecionista dos direitos dos indivíduos. É mister destacar uma característica comum e inerente a muitos crimes catalogados como de internet. Por esse motivo, relevante estabelecer considerações sobre a Transnacionalidade dessa modalidade criminosa.

2.6. Da Transnacionalidade dos Crimes Cibernéticos

Seguindo a regra trazida pelo Código Penal Brasileiro, o lugar do crime corresponde ao local onde seria gerado o resultado. No entanto, quando se depara com os delitos virtuais se torna muito difícil definir em qual local apropriado o crime se consumou.

A extrema dificuldade aqui mencionada é causada pela polaridade dos crimes de internet, uma vez que vítima e autor podem estar situados em lugares totalmente diversos, inclusive em países distintos.

Para Wendt[128] e Jorge "os recursos tecnológicos permitem que cibercriminosos, espalhados por diversas localidades, comuniquem-se e realizem ações criminosas em parceria organizadamente".

Dando continuidade a essa linha de pensamento, Wendt e Jorge[129] estabelecem que:

> "...essa interação do mundo com o uso de recursos tecnológicos por vezes dificulta a investigação de crimes, não pelo desconhecimento

[128] WENDT, Emerson. JORGE, Higor Vinícius Mendonça. **Crimes Cibernéticos**: Ameaças e Procedimentos de Investigação. Rio de Janeiro. Ed. Brasport, 2013, p. 181.
[129] WENDT, Emerson. JORGE, Higor Vinícius Mendonça. **Crimes Cibernéticos**: Ameaças e Procedimentos de Investigação. Rio de Janeiro. Ed. Brasport, 2013, p. 181.

> dos processos investigativos. A dificuldade ocorre quando o investigador se depara com o tráfego de pacotes que estão encriptados ou protegidos pelos provedores de conteúdo."

Na visão de Barreto[130], com a transnacionalidade dos crimes digitais é:

> "...extremamente difícil estabelecer com a clareza o local de consumação de um crime cibernético, especialmente em razão da ausência de fronteiras no ciberespaço.
>
> Os cibercrimes na grande maioria das vezes se caracterizam por serem plurilocais, quando vítima e agente estão em locais distintos, ou, ainda, quando a execução do delito se inicia em um lugar e a consumação ocorre em outro, mas no mesmo país.
>
> Caso a conduta criminosa seja praticada em um país e o resultado venha a ser produzido em outro, aplica-se o Art. 6º do Código Penal Brasileiro, que trata dos chamados crimes à distância."

Na medida em que a tecnologia se desenvolveu praticamente todas as atividades cotidianas puderam ser exercidas com o uso da rede mundial de computadores. Esse dinamismo alcançado pelas pessoas provocou uma maior vulnerabilidade e uma ampla suscetividade aos ataques provocados por criminosos virtuais.

A verdadeira problemática provocada pela transnacionalidade dos cibercrimes manifesta-se quando o resultado ocorre em um país e delitos, como divulgação de informações, ataques a honra e a servidores, por exemplo, têm seus autores localizados em outros territórios. Por sinal, prática que tem se tornado por demais corriqueira nessa modalidade criminosa.

Nessa esteira, Valin[131] aborda também essa problemática ao mencionar as questões de jurisdição e territorialidade, na sua visão:

> "...problema para a análise do caso quando a situação compreender a segunda figura da norma comentada, quando se considerar praticado o crime onde se produziu ou deveria produzir-se o resultado, principalmente com o que diz respeito aos crimes que podem ser cometidos com a divulgação de informações, ataque a servidores e furtos de dados."

---

[130] BARRETO, Alessandro Gonçalves/Brasil, Beatriz Silveira. **Investigação Cibernética,** à luz do Marco Civil da Internet. Rio de janeiro. Brasport, 2016, p. 25.

[131] VALIN, Celso. **A questão da jurisdição e da territorialidade nos crimes praticados pela internet**. Florianópolis: Boiteux, 2000, p. 116.

Em todo o mundo, na medida que foram crescendo e surgindo modalidade delitiva dessa espécie, os países foram obrigados a elaborarem leis que previssem certas condutas criminosas antes fora dos ordenamentos jurídicos pátrios. Ocorre que a carência de uma unidade legislativa, permitiu a ampliação da impunidade e com falta de cooperação internacional fizessem com que os crimes virtuais atraíssem ainda mais adeptos.

Segundo aponta Crespo[132] ao definir que não é o ciberespaço:

> "Propriamente um território, caracteriza-se especialmente pelo fluxo de informações por meios de redes de comunicação. Com isso, ganha importância a localização da informação, vez que é ela quem indica minimamente um território. É preciso considerar, ainda, que em muitos casos, os delitos cometidos nesse ambiente virtual possuem caráter transnacional, o que vai exigir dos países maior comprometimento no combate a esse tipo de criminalidade."

Ainda na visão de Crespo[133] a internacionalidade dos crimes de internet merece destaque, pois para ele:

> "os crimes digitais podem ser praticados parcialmente em diversos países, fragmentando-se o iter criminis. Questões sobre a presença física para a prática delitiva, bem como fronteiras territoriais ganham novas perspectivas, de modo que algumas características se mostram frequentes: a velocidade com o qual o delito é praticado, a distância a partir da qual se cometem os crimes, o volume de dados envolvido."

Na visão de Bezerra[134] diversos países já possuem legislações específicas para tratar as demandas relacionadas a crimes cibernéticos:

> "Certamente contam com a expertise de ações no sentido de tentar punir o delinquente deste tipo de delito, proporcionando um sentimento de segurança em sua sociedade. Observar, criticar, aprender e adaptar tais legislações é o caminho para se buscar a resposta ao crescimento vertiginoso do cibercrime."

Desta maneira, como forma de unificar diretrizes na elaboração legislativa e estabelecer uma cooperação técnica, os países europeus, EUA, Japão, Canadá,

---

[132] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais.** São Paulo. Saraiva, 2011, p. 117.

[133] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais.** São Paulo. Saraiva, 2011, p. 117.

[134] BEZERRA, Clayson da Silva/Agnoletto, Giovani Celso. **Combate ao Crime Cibernético.** Rio de Janeiro. Mallet Editora, 2016, p. 117.

Chile, Argentina, Paraguai, Austrália e República Dominicana se reuniram na cidade de Budapeste, Hungria. Essa reunião denominou-se de Convenção de Budapeste e visou uma política criminal comum a ser implantada nos diversos países signatários.

Como forma de esclarecer a classificação trazida pela Convenção de Budapeste, Barreto[135] estabelece:

> "Título 1 – Infrações contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos: acesso ilegítimo; interferência em dados; interferência em sistemas; uso abusivo de dispositivos.
>
> Título 2 – Infrações relacionadas com o conteúdo: infrações relacionadas com pornografia; burla informática.
>
> Título 3 – Infrações relacionadas com o conteúdo: infrações relacionadas com pornografia infantil.
>
> Título 4 – Infrações relacionadas com a violação do direito de autor e direitos conexos."

O Brasil participará do grupo como observador, devido a não conclusão do processo de adesão à Convenção de Budapeste. A entrada do país em definitivo permitirá um acesso mais rápido às provas eletrônicas que estejam no exterior, mediante cooperação jurídica internacional.

Devido a interconectividade, a troca de informações simultâneas e de dados vai muito além do território de um país. Dessa mesma forma acontece com os delitos cometidos por intermédio da web, pois o autor pode agir tranquilamente em um país vitimando pessoas que se encontram em outro, ou mesmo, é possível criar um vírus e disseminá-lo pela rede mundial afetando inúmeros sistemas informáticos em todo o mundo.

A transnacionalidade desses delitos dificulta o trabalho investigativo e a possível falta de cooperação internacional entre países permite que a legislação estrangeira sirva de entrave para o combate, identificação, e punição dos cibercriminosos.

Para um melhor combate aos crimes virtuais é necessário quebrar as amarras do Estado Constitucional Moderno que na visão de Cruz[136] seria:

---

[135] BARRETO, Alessandro Gonçalves/Brasil, Beatriz Silveira. **Investigação Cibernética,** à luz do Marco Civil da Internet. Rio de janeiro. Brasport, 2016, p. 23.

> "...aquele tipo de organização política, surgida das revoluções burguesas e norte-americana nos séculos XVIII e XIX que tiveram como principais características a soberania assentada sobre um território, a tripartição de poderes e a paulatina implantação da democracia representativa."

Somente um campo internacional comum em que possibilite a troca de informações, cooperação mútua e o uso de um direito transnacional nessa área é que poderá se alcançar melhores resultados na crescente ordem de crimes digitais.

Como bem explana Cruz[137]:

> "...a nova ordem mundial, influenciada por diversos fatores decorrentes da intensificação do fenômeno da globalização, torna oportuna e necessária discussão sobre a organização dos espaços públicos transnacionais, que viabilizem a democratização das relações entre estados, relação esta fundada na cooperação e solidariedade com intuito de assegurar a construção das bases e estratégias para governança, regulação e intervenção transnacionais."

Portanto, é necessário o rompimento com o Estado Constitucional Moderno para serem transpostas as fronteiras entre os países e combater com maior efetividade os crimes digitais de cunho transnacional. Um dos caminhos a serem percorridos é a cooperação técnica, já que a troca de informação, a divisão de conhecimento e a atuação conjunta são ferramentas importantes para se atingir resultados satisfatórios.

Um arcabouço legislativo sólido com cunho punitivo e abrangente quanto às inúmeras condutas cometidas pelos criminosos de internet também é um segundo caminho importante.

O estabelecimento de diretrizes após a Convenção de Budapeste é um excelente ponto de partida para se alcançar uma legislação conjunta, de forma a evitar que os diferentes tipos de leis façam que alguns países sejam mais atrativos para acolher criminosos desta espécie e permita que eles continuem praticando os delitos virtuais de cunho transnacional.

---

[136] CRUZ, Paulo/Stelzer, Joana. **Direito e Transnacionalidade.** Curitiba. Editora Juruá, 2009, p. 134.
[137] CRUZ, Paulo/Stelzer, Joana. **Direito e Transnacionalidade.** Curitiba. Editora Juruá, 2009, p. 134.

Logo, uma lei uniforme frente ao combate dos crimes cibernéticos desestimulará novos adeptos e didaticamente servirá de maneira preventiva a amenizar as consequências nefastas dessa crescente modalidade de delito.

2.7. Crimes Cibernéticos de maior incidência durante a Pandemia provocada pelo vírus da Covid 19

No ano de 2019, uma doença respiratória provocada pelo coronavírus denominado de Covid19 surgiu na China. O resultado da ação do vírus foi mortal e logo a transmissão se propagou do território chinês para todo o mundo.

O histórico do surgimento deste vírus mortal foi definido[138]:

> "...em meados de janeiro a imprensa começou a reportar casos sobre um "misterioso vírus que causava problemas respiratórios", tendo este vírus depois sido classificado como um coronavírus e chamado numa primeira fase de 2019-nCoV. Inicialmente, 800 pessoas foram infectadas e houve 259 mortes na China, mas houve casos também no Japão, Tailândia, Coreia do Sul, França e Estados Unidos, todos associados a pessoas que haviam viajado para a China recentemente. Em 20 de janeiro a OMS estimava que o número de casos poderia estar próximo de dois mil.
>
> Em 11 de março de 2020, o surto foi declarado uma pandemia, sendo que o número de casos confirmados a nível mundial atingiu mais de 121 000, sendo em 120 diferentes territórios, dos quais mais de 80 000 na China. O número de mortes ascende a 4 300, havendo mais de 1 200 mortes fora da China."

A necessidade de isolamento social como uma das formas preventivas de contrair o vírus fez com que pessoas pudessem adaptar seu cotidiano e adotar o trabalho na modalidade *home office*. Este motivo foi fundamental para um crescimento exponencial do acesso à web. A praticidade que já era vista por alguns passou a ser utilidade de todos. Literalmente a internet transformou-se em uma ferramenta de trabalho necessária e adotada por inúmeras empresas ao longo do mundo.

Na medida em que cresceu a acessibilidade, proporcionalmente houve um aumento significativo dos delitos virtuais. Naturalmente, devido ao enclausuramento das pessoas nas suas residências, os números de delitos

[138] https://pt.wikipedia.org/wiki/Coronavírus, acesso dia 29 de Novembro de 2021

praticados nas ruas como roubos, furtos, roubos a veículos e estelionato reduziram consideravelmente.

Contudo, os criminosos também tiveram que adequar suas estratégias para continuar no mundo do crime e a rede mundial de computadores foi o principal meio de acesso às vítimas. A quantidade de golpes eletrônicos (espécie de estelionato) e furtos por via eletrônica aumentaram significativamente, deixando clarividente a entrada de uma nova era que já era esperada, mas não para um futuro tão próximo.

O maior tempo despendido frente aos computadores e smartphones permitiu uma adesão ainda maior dos indivíduos às mídias sociais como Facebook, Instagram e Twitter. As relações pessoais diretas se distanciaram ainda mais, o que promoveu a comunicação por meio de aplicativos, chats e postagens. Junto a isso, vieram no primeiro plano a livre manifestação da opinião, enquanto no segundo plano se proliferaram as divergências de opiniões. Consequentemente, emergiram as ofensas contra a honra, sendo algumas diretas e outras fazendo uso de perfis falsos.

A criação de perfis falsos, prática criminosa de falsa identidade, foi também usada para que criminosos se passassem por pessoas ou empresas de alta influência nas redes sociais com o objetivo de disseminar conteúdos falsos, acarretando assim inúmeros prejuízos financeiros às empresas e a imagem de celebridades.

Uma espécie de crime digital praticado muito por cibercriminosos situados fora do país foram copiados por autores de delitos dentro do Brasil, cometendo o denominado “sequestro virtual”. Esse delito consiste no uso de programas maliciosos que conseguem o acesso remoto a computadores e smartphones, em seguida informações são retiradas e depois criptografadas, impedindo o acesso ao verdadeiro detentor dos dados. Ato contínuo os criminosos sob ameaça de não divulgar ou apagar as informações exigem o pagamento de uma quantia em dinheiro das vítimas.

Na visão de Cardoso[139]:

> "...inúmeros são os desafios e descobertas que fazem parte da nova realidade com a adoção mais intensificada da tecnologia, mas o imprescindível no mundo da tecnologia, é procurar manter-se sempre que possível atualizado, ou seja, ter o nosso antigo e precioso hábito que já temos fora do ambiente virtual, que é estar atualizado com as notícias, ter atenção, o cuidado ao sair nas ruas, ao falar com estranhos. As medidas de quem navega no ciberespaço, são as mesmas recomendadas de quem anda nas ruas. Inevitavelmente na mesma proporção que caminha os avanços no mundo digital, caminha também em alta os avanços do crime, criminosos que não dorme no ponto estão se evoluindo constantemente e atualizando com as tendências, aprimorando suas ferramentas cada vez mais poderosas para atacar, invadir, acessar indevidamente e obter dados e informações que sejam rentáveis."

Os crimes patrimoniais foram os mais adaptados durante a pandemia e novas formas de lesar o patrimônio alheio surgiram, seja pela dificuldade de identificação dos autores ou pela difícil recuperação dos valores subtraídos. Certamente, esses delitos patrimoniais à distância vieram para se instalar de forma definitiva.

A "clonagem" de WhatsApp, aplicativo de troca de mensagens, e a criação de auxílio emergencial falso foram os mais denunciados durante o ano de 2020. O primeiro consiste no uso de artifício ardiloso do meliante que pede à vítima para lhe passar um código enviado para o smartphone dela, em seguida já na posse desse código ele habilita a conta do WhatsApp da vítima e ativa a nova conta em um aparelho diferente, enviando mensagens para pessoas do contato pedindo dinheiro como forma de ajuda. Lamentavelmente achando tratar-se da vítima, pessoas acabam transferindo valores e prejudicando-se.

Nessa mesma linha, o golpe do auxílio emergencial falso foi criado como forma de aproveitar do momento em que o governo federal brasileiro disponibilizou, ao longo dos meses, certa quantia financeira como benefício para aqueles que seriam prejudicados por perder sua renda em razão da pandemia do coronavírus. Acontece que infratores antecipavam-se e criavam por aplicativo o cadastro de pessoas e indicavam uma conta distinta de titularidade do beneficiário, por fim

---

[139] CARDOSO, Nágila Magalhães. **A Pandemia do Cibercrime**. Porto Alegre, 2020, p. 19. Disponível em https://www.direitoeti.emnuvens.com.br/direitoeti/article/view/88/86 acessado em 15 de Novembro de 2020.

recebiam os valores e quando os reais necessitados tentavam fazer o cadastro frente ao governo federal descobriam que parte do benefício já tinha sido sacado e disponibilizado em uma conta bancária desconhecida da vítima.

A redução drástica do contato entre as pessoas para conter a propagação do vírus ampliou a procura pelos aplicativos de encontros virtuais. Com o fechamento de locais de lazer e entretenimento como bares, boates e casas de show, permitiu que o ambiente virtual se consolidasse como o único e mais seguro lugar para conhecer pessoas.

Diante disso, as trocas de intimidades por mensagens, fotos e vídeos cresceram significativamente. Aproveitando-se da ocasião meliantes passaram a se aproximar de pessoas para conseguir dados e informações de cunho pessoal, em seguida revelam seu real propósito exigindo dinheiro para não expor na rede mundial de computadores todas aquelas mídias digitais de cunho erótico ou até provocar um encontro sexual de forma chantageada.

A prática delitiva acima revelada recebeu o nome de sextorsão, que na visão de Barreto e Araújo[140] seria "forma de violência na qual o indivíduo, em razão de possuir conteúdo íntimo de terceiro, exige para não divulgação a contemplação lasciva ou a obtenção de outro material íntimo daquela pessoa".

De forma didática visando esclarecer essa nova modalidade de crime virtual, Barreto e Araújo[141] afirmam:

> "Na variável sextorsão, o autor, na posse de mídias digitais de conteúdo erótico da vítima, exige a prática de ato libidinoso para a não divulgação do material. O temor de uma exposição pública, do julgamento da sociedade e do apartheid social, obriga a pessoa, por vezes, a ceder a vontade do agressor. O dissenso da vítima, ou seja, a não concordância, diante da exigência de prática sexual é bem característico nessas formas de violência, pois há uma real perversidade no que tange à mulher e sua sexualidade".

Os autores Barreto e Araújo[142] continuam asseverando que "ao exigir a produção de mais material erótico digital como moeda de troca para a não

---

[140] BARRETO, Alessandro Gonçalves/Araújo, Vanessa Lee. **Vingança Digital**. Mallet Editora. Rio de Janeiro, 2017, p. 58.
[141] BARRETO, Alessandro Gonçalves/Araújo, Vanessa Lee. **Vingança Digital**. Mallet Editora. Rio de Janeiro, 2017, p. 58.
[142] BARRETO, Alessandro Gonçalves/Araújo, Vanessa Lee. **Vingança Digital**. Mallet Editora. Rio de Janeiro, 2017, p. 58

publicação do conteúdo íntimo da vítima, o agente promete causar mal grave, futuro e sério".

Esse período de crescimento dos delitos virtuais também serviu para o aumento do chamado ciberterrorismo que na visão de Falcão Junior e Buffon[143] seria "o terrorismo que consiste no uso de equipamentos de informática e da tecnologia da informação para o cometimento de atos danosos, com a finalidade de provocar o terror social ou generalizado".

O alvo comum do ciberterrorismo foram empresas e, principalmente, sobre o uso da vacina e de fármacos. A vacina sofreu um forte desincentivo do uso alegando malefícios e falsos efeitos colaterais. Já quanto aos fármacos, os ciberterroristas propagaram inúmeras inverdades de cura da doença provocada pelo coronavírus. A ideia central desses propagadores de falsas notícias é causar o caos e desestabilizar governos e desvalorizar ações de grandes companhias.

Seguindo a linha do propósito do ciberterrorismo, Falcão Junior e Buffon[144] asseveram:

> "O âmbito geográfico, o custo/benefício e a segurança pelo anonimato são algumas das grandes vantagens para a utilização da Internet para fins terroristas. O uso sofisticado do ciberespaço e das TICs permitem um aumento considerável no cometimento de delitos cibernéticos.
>
> Novas condutas surgem, com grande variação na forma de execução desses delitos, mas que não estão tipificadas em todos os países preocupados com o tema."

Por decorrência de uma demasia de delitos virtuais e um aparecimento de novas infrações penais, evidenciou-se a fragilidade e falta de técnica das policias investigativas em todo o mundo. A saída do campo real para o campo virtual demonstrou o quanto as técnicas investigativas precisam evoluir para encontrar as provas que possam demonstrar a existência delitiva, como também identificar a sua autoria.

---

[143] FALCÃO JUNIOR, Alfredo Carlos G./ Buffon, Jaueline Ana. **Crimes Cibernéticos**: Racismo, Cyberbullying, Deep Web, Pedofilia e Pornografia Infanto Juvenil, Infiltração de Agentes por Meio Virtual, Obtenção das Provas Digitais e Nova Lei Antiterrorismo. Porto Alegre. Livraria do Advogado, 2017, p. 155.

[144] FALCÃO JUNIOR, Alfredo Carlos G./ Buffon, Jaueline Ana. **Crimes Cibernéticos**: Racismo, Cyberbullying, Deep Web, Pedofilia e Pornografia Infanto Juvenil, Infiltração de Agentes por Meio Virtual, Obtenção das Provas Digitais e Nova Lei Antiterrorismo. Porto Alegre. Livraria do Advogado, 2017, p. 160.

Também abordando sobre a temática aqui mencionada, Falcão Junior e Buffon[145] destacam alguns problemas que os investigadores enfrentam quando precisam investigar o terrorismo cibernético:

> "a) complexidade técnica para a individualização das condutas;
>
> b) os cidadãos estão muito vulneráveis às ações criminosas;
>
> c) a diversidade de locais entre a execução da ação ilícita e o local atingido nessa atividade;
>
> d) falta de harmonia entre ordenamentos jurídicos nacionais;"

A transnacionalidade dos delitos cibernéticos facilitou muito a prática criminosa de autores situados em outros países. Percebendo que os brasileiros tem grande participação do seu tempo navegando na internet, com a frágil fiscalização e legislação repleta de lacunas, esses fatores que fizeram do país um campo perfeito para esse tipo de infrator virtual. Além disso, ampliou o intercâmbio entre cibercriminosos estrangeiros e os erradicados no Brasil, utilizando a *dark web* para troca de informações e conhecimentos maliciosos.

Mesmo com o fim da pandemia, acredita-se que os novos delitos permanecerão à medida que a tecnologia seguirá avançando ainda mais. Os Estados de uma maneira geral precisam investir consideravelmente em segurança da informação, corrigir suas legislações e preparar a sua polícia judiciária.

Crespo[146] assevera que é necessário:

> "...a cooperação internacional, promovendo intercâmbio de experiência em procedimentos de investigação e persecução em procedimentos judiciais, é outro aspecto imprescindível porque facilita sobre maneira a detecção de novas técnicas delitivas e a promoção da ação penal contra os criminosos."

A chegada da Covid 19 deixou às claras uma imensa lacuna legislativa por não prever diversos crimes de internet e, mesmo aquelas condutas já elencadas, demonstraram ser ineficazes pelas suas baixas e inócuas punições. A fragilidade legislativa exteriorizou ser necessário a elaboração de uma legislação comprometida

---

[145] FALCÃO JUNIOR, Alfredo Carlos G./ Buffon, Jaueline Ana. **Crimes Cibernéticos**: Racismo, Cyberbullying, Deep Web, Pedofilia e Pornografia Infanto Juvenil, Infiltração de Agentes por Meio Virtual, Obtenção das Provas Digitais e Nova Lei Antiterrorismo. Porto Alegre. Livraria do Advogado, 2017, p. 160

[146] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais.** São Paulo. Saraiva, 2011, p. 158.

na proteção de bens jurídicos e harmônica nos inúmeros países, como forma de garantir uma amplitude no combate desse tipo de infração.

Nessa linha de fundamento Crespo[147] destaca a importância de possuir um ordenamento jurídico mundial harmônico, senão vejamos:

> "Como necessidade conjunta, é preciso fazer estudo dos mecanismos penais em busca da implementação de soluções mais eficazes e com vistas a tornar o ordenamento jurídico mundial harmônico quanto a esses ilícitos, evitando que um Estado trate mais benevolente um delito. Não basta que um Estado incrimine uma série de condutas se estas serão vistas como indiferentes penais por outros Estados. E, nesse aspecto, apesar da complexidade, é preciso que as legislações sejam minimamente coerentes entre si para o combate aos crimes digitais."

Além de uma nova política de segurança de informação, os países devem aprofundar a educação digital, preparando os cidadãos com diversas técnicas preventivas como forma de evitar o comportamento vulnerável que expõe seus bens jurídicos e atraem os ataques virtuais. Assim, éticas informáticas são de grande valia a serem adotadas pelos usuários que compõem as diferentes classes sociais.

A nova mudança de paradigma trazida com a era digital, destaca os novos bens jurídicos e direitos que necessitam de uma proteção legal. Com isso, não é suficiente só municiar o direito penal, sem antes salvaguardar esses bens nas Constituições e nas demais normas infraconstitucionais.

Destarte, o longo período de duração dos efeitos trazidos pela pandemia leva a uma grande reflexão das entidades públicas, privadas e dos membros da sociedade. Mostrando que muito se tem a aprender com as adversidades surgidas e necessário se faz investir em políticas públicas, no fortalecimento legal e na mudança comportamental.

2.8. O uso de dados telemáticos na investigação dos crimes virtuais e a necessidade de relativização dos princípios da privacidade e intimidade

A revolução tecnológica trouxe uma diversidade de inovações tecnológicas que modificaram a vida das pessoas a tornando de certa forma mais

[147] **Idem.**

prática para um rol de tarefas antes realizadas com maior esforço e tempo empregado. Hoje, é possível ouvir músicas, participar de reuniões de trabalhos à distância, pagar contas bancárias, conversar ao mesmo tempo com um grupo de pessoas, tirar fotografias, gravar vídeos e áudios, etc. É possível observar uma distinção de atividades realizadas sob um único dispositivo.

Dispositivos tecnológicos como smartphones, palmtops, relógios inteligentes, entre outros, permitem uma facilitação das atividades e concentração destas em um único objeto eletrônico. Todavia, o telefone celular ao qual ganhou a nomenclatura de “smartphones”, telefones inteligentes, tornaram-se, nos dias atuais, o dispositivo eletrônico mais adquirido em todo o mundo e basicamente fundamental para a vida das pessoas. Tal dispositivo é usado pouco para sua função original, que é fazer ligações convencionais telefônicas, porém possui uma multitarefa, como fazer compras, trocas e-mails, mandar mensagens de voz ou escritas por meio de uma imensidão de aplicativos existentes, fazer transações bancárias, entre outras atividades cotidianas que todos realizam.

No presente momento, esses dispositivos vêm substituindo o computador convencional e sendo usado até mesmo como instrumento para prática criminosa. Através dele, infratores o utilizam para acessar a rede mundial de computadores e cometer uma diversidade de delitos que colocam em risco inúmeros bens jurídicos. A título exemplificativo, constata-se com maior frequência delitos contra à honra e contra o patrimônio, aos quais o aparelho celular vinculado à web é usado como “arma” para o cometimento desses crimes.

Por esse motivo, os dados armazenados no aparelho assumem um papel protagonista na busca de provas para o processo penal. Independente do bem jurídico tutelado, seja ele honra, patrimônio, vida, fé pública, entre outros, as informações contidas dentro da memória dos aparelhos celulares podem e são usados como meios de prova.

Vale lembrar que o aparecimento de aplicativos de trocas de dados através de aparelhos telefônicos, permitem mensagens de texto, de aúdio, chamadas equivalentes ao modo convencional, trocas de fotos e vídeos. Portanto,

tornaram-se a principal fonte para colaborar com a confirmação da materialidade e identificação de indícios de autoria.

A legislação brasileira permite a interceptação telefônica, de dados informáticos e de dados telemáticos como meio de captação de provas somente a ser autorizada judicialmente na sua forma excepcional e para alguns crimes específicos cometidos. Por outro lado, o acesso a conversas, áudios, e dados contidos em dispositivos eletrônicos consiste uma violação à privacidade e à intimidade do indivíduo, direitos estes resguardados constitucionalmente.

Enquanto os aplicativos se aperfeiçoam para restringir ainda mais o acesso de terceiros às informações privadas, aqueles detentores destes direitos recorrem ao Poder Judiciário para impedir ou anular provas obtidas pela polícia investigativa. Sob outro cenário, os representantes do Estado tentam priorizar a ordem pública e os agentes policiais se aprimoram em buscar técnicas de coleta de dados e informações como meio de prova.

No rol de direitos constitucionalmente previstos estão os da privacidade e intimidade, aos quais possibilitam que as relações interpessoais, vida privada e dados individuais sejam conservados e acessíveis somente com autorização do próprio detentor do direito. Entretanto, como uma série de direitos elencados na Constituição Federal Brasileira, promulgada em 1988, esses direitos não são absolutos, e excepcionalmente, podem ser relativizados, desde que sejam previamente autorizados pelo Poder Judiciário com o fim de atender a um interesse público.

É possível se extrair da atual Constituição Federal[148] que:

> 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:
>
> I – [...]

---

148 **CONSTITUIÇÃO FEDERAL**, acessado em www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

> 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;

No sentir do constitucionalista Moraes[149] os direitos aqui apontados figuram como direitos humanos fundamentais a todo cidadão, por isso assevera que seria

> [...] como o conjunto institucionalizado de direitos e garantias do ser humano que tem por finalidade básica o respeito a sua dignidade, por meio de sua proteção contra o arbítrio do poder estatal e o estabelecimento de condições mínimas de vida e desenvolvimento da personalidade humana.

Uma rápida análise ao texto constitucional deixa clarividente que a vida privada, honra, imagem e intimidade são direitos invioláveis e a violação a elas direcionada enseja em indenização pelo dano material e moral. Como já exposto, não se pode fazer uma interpretação restritiva desta passagem da Constituição Federal brasileira, uma vez que merece destaque que não se tratam de direitos absolutos e sua relativização depende de cláusula de reserva de jurisdição. Contudo, é plenamente possível a quebra da imutabilidade, quando houver caráter excepcional e extrema necessidade devidamente comprovada.

Bastos e Martins[150] ao tecerem comentários ao inciso X, do Art. 5º da Constituição Pátria estabelecem que:

> "O inciso oferece guarida ao direito à reserva da intimidade assim como ao da vida privada. Consiste na faculdade que tem cada indivíduo de obstar a intromissão de estranhos na sua vida privada e familiar, assim como impedir-lhes o acesso a informações sobre a privacidade de cada um, e também impedir que sejam divulgadas informações sobre esta área da manifestação existencial do ser humano".

Em busca de um entendimento mais preciso da intimidade como direito constitucionalmente resguardado ainda se faz necessário definir alguns conceitos

---

[149] MORAES, Alexandre de. **Direitos humanos fundamentais**: comentários aos arts. 1º ao 5º da Constituição da República Federativa do Brasil. São Paulo: Atlas, 1997, v. 3, p. 39.
[150] BASTOS, Celso Ribeiro; MARTINS, Ives Gandra da Silva. **Comentários à Constituição do Brasil**. São Paulo: Saraiva, 1989, v. 2, p. 63.

para melhor compreender o peso do seu afastamento momentâneo frente a outros interesses. Por isso, na visão de Da Silva[151] esse direito:

> "[...] deve compreender o poder jurídico de subtrair ao conhecimento alheio e de impedir qualquer forma de divulgação de aspectos da nossa vida privada, que segundo um sentimento comum, detectável em cada época e lugar, interessa manter sob reserva".

Na mesma linha de entendimento De Cupis[152] define o direito à intimidade como:

> "[...] protetor de um modo de ser pessoal, que exclui os outros do conhecimento da esfera mais intensa e pessoal do indivíduo. Essa exclusão de conhecimento obedece à necessidade de afastamento da vida íntima do universo da comunicação".

É cediço que com o avanço tecnológico os smartphones passaram a ser instrumento cada vez mais importante na vida das pessoas. Como explanado, a gama diferenciada de atividades realizadas por este dispositivo eletrônico faz com que o seu proprietário estabeleça um controle ainda maior do seu acesso e restrinja de toda forma a exposição de seu conteúdo.

Então, necessário se faz elaborar um questionamento: Quais instrumentos devem ser utilizados quando uma informação de suma importância para a persecução penal, seja para comprovar a materialidade de um delito ou apontar sua autoria, encontra-se dentro desse dispositivo? Indagação a ser realizada que gera forte discussão dentro do meio acadêmico e também no corpo dos tribunais, dividindo-se entre os protetores dos direitos privados, como já abordado, respaldados constitucionalmente, em outra face os publicistas que colocam o interessa da sociedade em primeira mão.

Conforme destacado alhures, exceto o direito à vida, não há que se mencionar em direito constitucional absoluto conferido ao homem e, sobre essa ótica, os que atuam em busca da verdade real adotam esse argumento. Sabe-se que a privacidade deve ser preservada e garantida constitucionalmente, cujo no mesmo rumo atuam as normas infraconstitucionais. Entretanto, quando outros bens

---

[151] DA SILVA, Edson Ferreira. **Direito à Intimidade**. São Paulo: Ed. Oliveira Mendes, 1998, p. 39.
[152] DE CUPIS, Adriano. **Os Direitos de Personalidade**. São Paulo: Ed. Romana,2004, p. 283.

jurídicos pertencentes a terceiros estão em risco, se deve fazer um juízo de valoração e priorizar a flexibilização do seu acesso, não permitindo o alcance da impunidade e afastando barreiras em demasia à atuação estatal.

A flexibilização aqui defendida, deve ser permissiva somente às informações pertinentes à atividade investigativa e de interesse exclusivo ao processo penal, permitindo o acesso exclusivamente às partes diretamente envolvidas na persecução penal, de modo que seja imposto o sigilo não possibilitando o acesso àqueles outros que não figuram como atores no âmbito processual.

Sendo assim, os direitos à intimidade e privacidade do investigado não serão de certa forma desrespeitados, ou mesmo, afastados. Embora alguns adeptos da interpretação restritiva da norma assim entendam. Portanto, a quebra do acesso restrito das informações pertencentes a uma pessoa será palpável somente para um número de pessoas extremamente restritas que figurarão dentro do processo penal como parte atuante.

Não se deve olvidar que os servidores ao qual violam sigilo funcional, propagando conteúdo existente nos autos ao qual o próprio julgador estabeleceu sigilo, cometem delito previsto no Art. 10[153] da Lei 9296/96, Lei de Interceptação Telefônica, ao qual elenca que:

> "Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, promover escuta ambiental ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei: (Redação dada pela Lei nº 13.869. de 2019)
>
> Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa. (Redação dada pela Lei nº 13.869. de 2019)"

Logo, a própria legislação especial prevê pena de reclusão de 2 a 4 anos para os descumpridores da manutenção do sigilo das informações existentes no bojo do processo, constatando assim mais um instituto protetivo aos direitos à privacidade e à intimidade.

---

[153] **LEI DE INTERCEPTAÇÃO TELEFÔNICA**. Acesso realizado em http://www.planalto.gov.br/ccivil_03/leis/l9296.htm

Em observância ao marco civil da internet, lei 12.965/14, mais precisamente no seu Art. 3º[154], quando se menciona sobre acesso à internet, a própria lei arrola direitos aos quais devem ser respeitados e preservados, dentre eles estão a proteção à privacidade e dos dados pessoais.

> 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;
> 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.

Os dados telemáticos dependem de um sistema de redes para sua transmissão, como a internet que é uma rede pelo qual esses dados podem ser transmitidos, sendo assim é possível concluir que tais informações estão tuteladas pela lei ora citada e, por conseguinte a privacidade e dados pessoais neles contidos.

O Marco Civil da Internet dispõe que a guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet, de dados pessoais e do conteúdo de comunicações privadas devem atender à preservação da intimidade, da vida privada, da honra e da imagem.

Ilustrando tal afirmação do parágrafo anterior, se pode observar no Art.7º[155] do Marco Civil da Internet a proteção à esses direitos, senão vejamos:

> 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;

---

[154] **Marco Civil da Internet**. Acesso realizado em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

[155] **Marco Civil da Internet**. Acesso realizado em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

> 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;

Visando definir o real propósito desta lei, Bergmann[156] assevera que:

> "Apesar de o texto aparentar proteger os usuários da internet de ameaças às suas liberdades e vida privada quando praticadas pelo Estado, como se este fosse o maior interessado em violá-las, o fato é que até mesmo os que defenderam a total ausência do controle e guarda de registros na utilização da internet agora clamam por punição aos que se utilizam da rede para praticar toda a sorte de delitos, como racismo, injúria, fraudes eletrônicas, pornografia infantil, etc"

Após algumas considerações acerca do diploma que explana sobre a internet, necessário se faz definir o conteúdo que transita nesta rede mundial de computadores. Nesse passo, é possível dizer que telemática seria a junção palavras telecomunicação com informático, assim dizendo que é a tecnologia que permite a comunicação à distância entre serviços de informática e redes de telecomunicações.

Todas as informações que constituem o sigilo telemático são regidas por diferentes leis, mais especificamente a Lei n. 9.296/96 (Lei de Interceptação das Comunicações Telefônicas, Telemáticas e Informática) e a Lei n. 12.965/14 (Marco Civil da Internet) que regulam dados telefônicos e da internet, respectivamente.

Destarte, os dados telemáticos em mãos erradas podem tornar-se uma poderosa "arma" causadora de extrema devassa na vida privada e profissional de alguém, uma vez que grande quantidade de informações que compõem seu

[156] BERGMANN,Pablo Barcellos. **Aspectos Penais do Marco Civil da Internet**. IN Combate ao Crime Cibernético. Mallet: Rio de Janeiro, 2016, p. 46/47.

conteúdo podem revelar aspectos íntimos que não se desejava revelar. Por outro lado, podem ser de grande valia para nortear uma linha investigativa e servir de forte arcabouço probatório.

A plenitude do exercício de direitos como privacidade e intimidade é garantia pela atual Carta Magna de 1988. Tomando por base essa proteção, os usuários de computadores, smartphones e outros aparelhos eletrônicos utilizam esses dispositivos com maior tranquilidade, seguros de que suas informações privadas ali expostas estarão resguardadas e distante da curiosidade alheia.

Hodiernamente, os direitos ora citados são classificados como fundamentais, que na visão de Sarlet[157]:

> "...também se apresentam como dever de proteção do Estado, que deve agir de maneira preventiva na proteção dos particulares diante dele próprio (o Estado) e dos demais particulares. A valorização dos direitos fundamentais na perspectiva objetiva resultou na conscientização da insuficiência de uma concepção dos direitos fundamentais como direitos subjetivos de defesa para a garantia de uma liberdade efetiva para todos, e não apenas daqueles que garantiram sua independência social e o domínio de seu espaço de vida pessoal."

Levando por base essa segurança, criminosos aproveitam certa situação garantista para trocar mensagens, fotos, aúdios e vídeos abarcando uma grande diversidade de delitos. Após a pandemia provocada pelo coronavírus, o número de pessoas que passaram a acessar a rede mundial de computadores atingiu quase toda a totalidade da população brasileira, juntamente com isso houve a multiplicação de crimes cibernéticos, principalmente aqueles voltados para o bem jurídico patrimônio.

Some-se a isso que as diferentes espécies de tráfico como de drogas, de armas, de pessoas, de órgãos e de animais, etc, utilizam os diversos aplicativos de mensagens para trocar informações a respeitos desses delitos.

Diante disso, como alegar que os direitos a privacidade e intimidade previstos constitucionalmente são absolutos, ou seja, alheios ao acesso de terceiros.

---

[157] SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**. 7. ed. Porto Alegre: Livraria do Advogado, 2007, p. 177.

Pois, de que forma ficaria o interesse público, a segurança da coletividade e a garantia da segurança pública? Questionamentos que necessitam ser feitos diante da contraposição entre direitos previstos na Carta Magna Brasileira.

Por esse motivo, o princípio da proporcionalidade deve ser evocado para resolver certo conflito entre interesses e direitos, balizando como melhor aplicar a norma constitucional sem ofender literalmente os bens jurídicos dos cidadãos. Sobre essa linha de pensamento, Pulido[158] explana:

> "Na aplicação do princípio da proporcionalidade aos direitos fundamentais, deve-se considerar a faceta da proibição da proteção deficiente. Ao intérprete, caberá aferir se uma atuação estatal, por ação ou omissão, torna vulnerável um direito fundamental. Por meio da proibição de proteção deficiente, permite-se a fixação de um padrão mínimo de proteção aos direitos fundamentais que deve ser observado e promovido pelo Poder Público."

De certa forma, é possível estabelecer que os direitos individuais aqui citados são como obstáculos impostos ao Judiciário que demandam uma sensível análise dos pedidos que lhe são direcionados para dá cabo à persecução penal em sua plenitude no uso de técnicas investigativas. Nesse sentido, Tucci[159] elenca:

> "...os proclamados direitos do indivíduo integrante da comunidade põem-se como autênticas barreiras contra a atuação dos agentes estatais da persecução penal e dos órgãos do Poder Judiciário, limitando-a no interesse da privacidade, cuja asseguração constitui exigência inarredável do Estado de Direito. Mas o Estado, no exercício do poder-dever de punir, no curso da persecução penal, pode limitar a tutela da intimidade e da vida privada do indivíduo, nos termos da Lei Maior."

Em primeira mão, é necessário se aprender às técnicas de coleta de informações não ofensivas aos direitos individuais. Todavia, quando os agentes de polícia judiciária se deparam com a impossibilidade de uso das técnicas menos invasivas, é preciso dá um próximo passo rumo à coleta segura de vestígios e,

---

[158] PULIDO, Carlos Bernal**. El principio de proporcionalidad y los derechos fundamentales.** 4. ed. Bogotá: Universidad Externado de Colombia, 2014, p. 173.

[159] TUCCI, Rogério Lauria. **Direitos e garantias individuais no processo penal brasileiro**. Tese para concurso de Professor Titular de Direito Processual Penal da Faculdade de Direito da Universidade de São Paulo. São Paulo: Saraiva, 1993, p. 419.

nesse momento, com a relativização da intimidade e privacidade se podem alcançar os dados essenciais que embasarão o inquérito policial e a futura ação penal.

Corroborando essa linha de pensamento, Aragão[160] afirma:

> "... a crescente utilização dos meios digitais para a prática de crimes ou a presença de vestígios nessas plataformas que possam elucidar a autoria e a materialidade delitiva, tem-se como razoável o afastamento do direito à privacidade para a investigação criminal, prevalecendo o dever do Estado de promover a persecução penal em face do direito individual do investigado de ter sua privacidade resguardada. Mas é preciso analisar o caso concreto para saber se é necessária a autorização judicial para o desenvolvimento da técnica investigativa, bem como se não há outro meio disponível para a coleta da prova."

Objetivando exemplificar a não plenitude de direitos do indivíduo e destacando a possibilidade de afastamento de certas garantias Moraes[161] atribui que:

> "A interpretação do presente inciso deve ser feita de modo a entender que a lei ou a decisão judicial, poderão, excepcionalmente, estabelecer hipóteses de quebra das inviolabilidades da correspondência, das comunicações telegráficas e de dados, sempre visando salvaguardar o interesse público e impedir que a consagração de certas liberdades públicas possa servir de incentivo à prática de atividades ilícitas. No tocante, porém, à inviolabilidade das comunicações telefônicas, a própria Constituição Federal antecipou-se e previu requisitos que deverão, de forma obrigatória, ser cumpridos para o afastamento dessa garantia."

No mesmo diapasão, Gomes e Cervini[162] afirmam:

> "A questão central, segundo o constitucionalismo moderno, não é se o legislador pode ou não restringir direitos, senão se sua intervenção se dá dentro de limites excepcionais e proporcionais. Algumas normas constitucionais preveem, expressamente, a possibilidade de limites a direitos fundamentais (caso típico é o inciso XII em pauta). Outras normas não contam com a previsão de restrição. Nem por isso, foi restabelecida a doutrina dos direitos absolutos. Não existem direitos absolutos. Nem sequer o direito à vida, que é o mais relevante, é totalmente intangível."

---

[160] ARAGÃO, David Farias de. **Limites constitucionais e efetividade da investigação criminal de delitos cibernéticos**. IN Combate ao Crime Cibernético. Mallet: Rio de Janeiro, 2016, p. 225.

[161] MORAES, Alexandre de. **Direitos Humanos Fundamentais** - Teoria Geral . São Paulo: Atlas. 2011, p. 240.

[162] GOMES, Luiz Flávio; CERVINI, Raúl. **Interceptação telefônica**. São Paulo: RT, 1997, p.71.

Ao abordar sobre a coleta de dados telemáticos, estabelecendo e destacando sua importância. Há de se notar seu amparo legal em total consonância com a atual Constituição Federal Brasileira ao qual recepciona perfeitamente o dispositivo de lei especial que aborda sobre as interceptações telefônicas e se coaduna com a interceptação também de dados telemáticos. Nesse espeque, o mestre Damásio Evangelista de Jesus[163] denota:

> "Inclinamo-nos pela constitucionalidade do referido parágrafo único. A Carta Magna, quando excepciona o princípio do sigilo na hipótese de 'comunicações telefônicas', não cometeria o descuido de permitir a interceptação somente no caso de conversação verbal por esse meio, isto é, quando usados dois aparelhos telefônicos, proibindo-a, quando pretendida com finalidade de investigação criminal e prova em processo penal, nas hipóteses mais modernas. A exceção, quando menciona 'comunicações telefônicas', estendesse a qualquer forma de comunicação que empregue a via telefônica como meio, ainda que haja transferência de 'dados'. É o caso do uso do modem. Se assim não fosse, bastaria, para burlar a permissão constitucional, 'digitar' e não 'falar'."

Assim sendo, essencial se faz o uso do princípio da proporcionalidade frente à colisão de direitos públicos e privados, porém o uso em demasia, ou seja, a imutabilidade de direitos privados, como da privacidade e intimidade, possibilita que criminosos utilizem essa proteção para cometimento de diferentes delitos e, quando necessário, avocarem garantias constitucionais para continuar no universo da criminalidade e se esquivando do *jus puniendi* estatal. Em outra face, a plenitude dos direitos públicos como segurança pública e interesse público, concede pleno poder ao Estado, permitindo que as instituições que agem em seu nome "atropelem" em demasia os direitos individuais.

Destarte, somente a relativização dos direitos constitucionais inerentes ao indivíduo com uma atuação conjunta do princípio da proporcionalidade, se atingirá um equilíbrio para que instituições atuantes na esfera da investigação possam usar os mecanismos legais para identificação de autores de delitos e produção de prova da materialidade delitiva.

---

[163] **JESUS,** Damásio Evangelista de. Interceptação de comunicações telefônicas: notas à Lei nº 9.296, de 24.07.1996. Revista dos Tribunais, São Paulo, 1997.

Feitas essas considerações sobre as características, peculiaridades e legislação dos crimes virtuais, salutar explicitar sobre os desafios da atividade investigativa para conseguir reunir provas e identificar os autores dessa forma especial de delito. Da mesma forma, é de suma importância descrever quais são os crimes digitais mais corriqueiros no presente momento e quais técnicas investigativas podem ser adotadas pelos agentes de polícia judiciária no tocante ao combate e elucidação dessa estirpe de infração penal. Temáticas que serão abordadas no capítulo seguinte.

CAPÍTULO 3

OS DESAFIOS NA INVESTIGAÇÃO DOS CRIMES CIBERNÉTICOS E O USO DAS MELHORES TÉCNICAS INVESTIGATIVAS E PROCEDIMENTAIS PARA IDENTIFICAÇÃO DE AUTORIA E FORMAÇÃO DE PROVAS PARA O COMBATE DESSA MODALIDADE DELITIVA

3.1. Dos desafios enfrentados pela polícia judiciária frente aos delitos virtuais

A dinâmica social dentro da sua efemeridade exige das mais variadas atividades uma adaptação continua. Não muito distante disso encontra-se a atividade investigativa que precisa está sempre em acompanhamento às mudanças sociais e principalmente às novas modalidades criminosas que atingem diretamente as pessoas.

Dentro desse prisma, a ampla acessibilidade aos novos aparatos tecnológicos possibilitou a alteração dos meios para a prática dos delitos tradicionais, como ao mesmo tempo fez surgir novas tipologias delitivas. Nesse contexto, surgiram os delitos denominados de digitais que a cada dia atingem um número ainda maior de vítimas.

Conforma assevera Teixeira[164], alguns elementos como

> "...o avanço das novas tecnologias impulsionando a globalização, a popularidade da Internet proporcionando conveniência aos usuários e a co-circulação de comércio eletrônico, dinheiro e informações, a Internet tornou-se um ambiente atraente para criminosos."

Na visão de Lorusso[165] outros aspectos contribuem para o fenômeno dos crimes virtuais:

> "... il mondo underground dela criminalità informática, poi, há rapidamente compreso come la stesura di codici maligni possa di fato aprire la strada ad enorme opportunità per la realizzazione di elevati guadagni, molte dele minacce telematiche atualmente sviluppate por essere poi vendute ad altri malintenzionati. Il crimine è ormai um

[164] TEIXEIRA, T. **Direito Digital e Processo Eletrônico**. 1 ed. São Paulo: Editora Saraiva, 2020, p. 209.
[165] LORUSSO, Piero. **L'insecurezza dell'era digitale**: Tra cybercrimes e nuove fronteire dell'investigazione. Confini Sociologici. Franco Angeli. Milano, 2011, p. 08.

> fenômeno connaturato alla società moderna e tocca ogni aspetto della nostra vita..."

O grandioso desafio para as polícias judiciárias de todo país paira sobre como melhor atender essa grande demanda, protegendo os variados bens jurídicos, restabelecendo o status anterior das vítimas, quais as técnicas investigativas a serem adotadas para identificação da autoria e comprovação da materialidade do crime.

De certa forma, o comportamento da própria população propicia um cenário favorável para a propagação dos delitos digitais. Conforme afirma Silveira[166]:

> "A Sociedade da Informação é, por defeito, uma sociedade vulnerável. Por um lado, as características do meio informático propiciam e facilitam a actividade delituosa; por outro lado, a actividade de prevenção, investigação e repressão dessa criminalidade tem-se tornado cada vez mais difícil, pelo que vulnerabilidade e a probabilidade de impunidade torna o ambiente informático ainda mais atraente. Torna-se, assim, imprescindível que o Direito Penal e o Direito Processual Penal acompanhem esta evolução tecnológica, que se traduz numa eminente modernização da criminalidade, de forma a garantir uma resposta eficaz aos desafios que esta sociedade digital lhes coloca..."

Nitidamente pela ausência de expertise com a matéria e diante dos inúmeros obstáculos que estão por trás dos delitos cibernéticos, nota-se um desinteresse na atividade investigativa e uma descrença da população na solução desta modalidade de ilícito penal, e como consequência, há um baixo grau de resolutividade dos delitos.

A capacitação deficitária ou insuficiente não permite que os agentes policiais acompanhem a dinâmica dos novos crimes e com isso, na medida em que a tática criminosa chega ao conhecimento do público em geral, sem ninguém ter sido processado, em um breve espaço de tempo, os cybercriminosos já utilizam de nova estratagema para alcançar mais vítimas. Enfim, devido à impunidade já alteram o *modus operandi* e dão continuidade a sua saga delituosa.

Na visão de Rosendo[167]:

---

[166] SILVEIRA, Maria Ana Barroso de Moura da. **Da problemática da Investigação Criminal em Ambiente Digital** - em especial, Sobre a Possibilidade de utilização de malware como meio oculto de obtenção de prova. Mestrado Forense, Lisboa, 2016, p. 07.

> "Faz-se necessária uma mudança de postura com relação ao sistema investigatório brasileiro, sistema este, que se encontra em crise e mal visto pela sociedade. Os altos índices de criminalidade no país refletem a necessidade de uma reforma na nossa legislação, de forma a adaptá-la a realidade encontrada atualmente, desvinculando-se de características que em muito contradiz a Constituição Federal garantista que adotamos."

Acrescentando a isso, a ausência de técnicas específicas e de um modelo padrão no combate dos crimes virtuais, colocam esses crimes como os mais frequentes e de maior número. A percepção dos criminosos com a possibilidade de agir à distância sem ser "pegos", ou melhor, presos e processados, permitem que "pseudos crackers" com rasteiro conhecimento na área passem a optar por esse tipo de crime, pela mínima chance de ser responsabilizado penalmente. Logo, a falha estatal permite uma onda de crescimento dos delitos e uma migração dos criminosos para o ambiente virtual.

A deficiência ora apontada demonstra que o Estado precisa investir não só na capacitação do seu pessoal, como necessita investir em aparatos tecnológicos que contribuam para rastrear criminosos e preservar material probatório.

As carências apontadas têm levado uma enxurrada de transferências dos boletins de ocorrências que envolvam crimes virtuais para as novas delegacias de crimes cibernéticos. A alta demanda tem prejudicado a dedicação das novas delegacias especializadas em combater crimes digitais de alta complexidade que atinjam uma grande quantidade de vítimas e cause significativo impacto social.

Por isso, é urgente a necessidade de disseminação de novas técnicas para os membros das polícias judiciárias, para aprimorar sua atuação e ampliar o combate aos novos criminosos, permitindo que a ampla sensação de insegurança, quando se fala do ambiente virtual, seja reduzida.

Para Castro[168]:

---

[167] ROSENDO Juliana Vital; CARVALHO Grasielle Borges Vieira de; **Os novos desafios e perspectivas acerca da investigação criminal no Brasil.** Cadernos de Graduação. Aracaju, 2015, p. 73.

[168] CASTRO, Inês Maria Vaz Prego de**. O contributo da Polícia Judiciária na Investigação Criminal e a Cooperação Policial.** Mestrado Forense. Lisboa, 2016, p. 10.

> "...é vital centralizar, tratar e analisar a informação criminal especulativa. Só através do trabalho de recolha sistemática de informação se consegue alcançar um eficiente combate ao crime. Para além disso, a investigação criminal dos dias de hoje implica a existência de estruturas organizacionais altamente especializadas, com elevados níveis de eficácia e de capacidade de resposta, dotadas de meios adequados..."

É possível vislumbrar que delitos como a disseminação não autorizada de fotografias íntimas, a sextorsão e o estelionato eletrônico continuem numa crescente devido ao ambiente virtual ser ainda um campo propício onde os atacantes militam sem ser afetados.

A carência de conhecimento dos agentes policiais nessa seara é tamanha que mesmo os criminosos com uma gama de conhecimento rasteiro conseguem ficar no âmbito da clandestinidade sem ser identificados e detidos. O uso de técnicas simples e de forma padronizada permitiria um aumento significativo no número de resolução dos crimes cibernéticos, reduzindo ao mesmo tempo o campo de obscuridade que permeia dentro dessa espécie delitiva.

Sem sombra de dúvidas, um maior investimento em aparato tecnológico, uma disseminação maciça de conhecimento nessa área e um aumento da instauração dos procedimentos investigativos permitirá a identificação de muitos criminosos e sua consequente responsabilização penal, tudo isso, possibilitará não só a ampliação da proteção da sociedade como aumentará a credibilidade das polícias civis de todo o país.

3.2. Os delitos cibernéticos mais comuns no momento atual e as técnicas utilizadas para identificação da autoria e materialidade

Ad initio, antes de tecer alguns pormenores sobre os delitos mais corriqueiros dentro de um cotidiano e detelhar técnicas de combate a eles, necessário se faz destacar que o presente trabalho não menciona todo e qualquer delito praticado pela internet, nem mesmo esgota todas as técnicas investigativas possíveis.

Logo, há uma intenção de demonstrar como os crimes virtuais que alcançam mairo número de vítima pode ser explorado pela polícia judiciária no seu exercício da persecução penal, qual o norte a ser tomado e demais passos iniciais rumo a identificação dos atacantes e ofensores dos direitos fundamentais do indivíduo e como melhor atuar para preservar todos elementos de informação ali presentes para possibilitar que sejam aproveitados como prova dentro de uma instrução criminal.

3.2.1. Sextorsão e as técnicas adotadas para investigação criminal

Ao observar os delitos virtuais mais corriqueiros, depois dos diversos diferentes tipos de fraudes eletrônicas que geram prejuízos financeiros às vítimas, verifica-se uma modalidade de crime digital que afeta o patrimônio conhecida como sextorsão.

É possível afirmar que se entende como uma espécie do gênero extorsão, crime que tutela o patrimônio e a liberdade individual, alocado no Art. 158[169] do Código Penal Brasileiro:

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

Sydow e Castro[170] definem a sextorsão como:

> "... trata da figura em que uma relação de poder é utilizada como instrumento para obter vantagens sexuais. É uma modalidade de conduta não adequadamente definida na legislação nacional por

[169] **CÓDIGO PENAL BRASILEIRO**, https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm, acesso em 03/08/2022.
[170] SYDOW, Spencer Toth; CASTRO, Ana Lara Camargo. **Sextorsão.** Vol. 959. Revistas dos Tribunais, 2015, p. 01.

> conjugar uma corrupção individual com um abuso de poder no intuito de obter sexo em troca de benefícios. Com a propagação da informática, novos modos de extorsão a partir da ameaça de divulgação de fotos e filmes tem se difundido com grande força."

A autora D'Urso[171] pontua que a sextorsão:

> "...cujo termo consiste na união da palavra sexo com a palavra extorsão, e se caracteriza como uma chantagem online pelo constrangimento de uma pessoa à prática sexual ou pornográfica registrada em foto ou vídeo para envio, em troca da manutenção do sigilo de seus nudes, previamente armazenados por aquele que faz a ameaça."

Apesar da definição explanada pelos autores versar sobre o intuito desse tipo de extorsão objetivar favores sexuais, não se pode olvidar que se está diante de um delito que atinge o patrimônio e muitos cybercriminosos agem com o intuito de conseguir vultuosos valores financeiros para não propagar as íntimas fotos em rede social e findar por expor a vítima, e, consequentemente, provocar abalos psicológicos e afetar de alguma forma a relação familiar.

Destarte, essa espécie de extorsão pode ir muito além do patrimônio e da liberdade individual, afetando também psicologicamente aqueles que são chantageados e atingir a imagem e privacidade dos envolvidos.

Nesse diapasão, os autores Sydow e Castro[172], corroborando com a ideia acima, destacam:

> "A sextorsão encontra na era tecnológica um imenso propulsor de coerção psicológica, que beneficia os autores e apavora as vítimas, uma vez que o potencial de difusão e de danos à intimidade é incalculável. Dessa forma, tanto a vítima que na sextorsion conceitual cede ao abuso de poder e se submete à pratica sexual, sendo então fotografada ou filmada, permanecerá nas mãos do explorador, quanto à vítima da sextorsion das relações cotidianas será mantida sob permanente controle."

---

[171] D'URSO, Adriana Filizzola, **Sextorsão e Estupro Virtual:** Novos Crimes Na Internet. São Paulo,2017, p. 01. http://www.cjlp.org/materias/ARTIGO%20%20Sextorsao%20e%20Estupro%20Virtual_Adriana_Filizzola_DUrso.pdf. Acesso em 06 de Dezembro de 2022.

[172] SYDOW, Spencer Toth; CASTRO, Ana Lara Camargo. **Sextorsão.** Vol. 959. Revistas dos Tribunais, 2015, p. 08/09.

Os infratores, na maioria dos casos, usam um perfil falso e utilizam locais de bate papo na web para se aproximar das vítimas, em outros casos, solicitam para ser adicionados como amigo no facebook ou instagram e a partir disso iniciam um contato mais próximo. Depois de adquirir confiança vão muito mais além e fazem inúmeras promessas para ampliar esse grau de confiabilidade e, posteriormente, iniciar um relacionamento virtual.

Os passos seguintes podem variar, pois pode ser enviado um malware para invadir o dispositivo eletrônico da vítima (smartphone ou notebook) e conseguir acesso a vídeos e fotos, como também há o uso de conversa ardilosa para conseguir fotos e vídeos de cunho íntimo da vítima, nesse último caso a própria vítima após ser ludibriada finda por enviar material de cunho íntimo.

Sem menos esperar, a pessoa recebe proposta em dinheiro ou ordem para gravar vídeos ou mesmo tirar mais fotos e enviar para o infrator, sempre sobre ameaças de colocar o material a disposição da família ou de contatos existentes nas redes sociais da vítima.

Bernardo e Prado[173] explanam que os autores nesse tipo de crime agem:

> "Em alguns casos, as exigências são relacionadas ao envio de novas fotos ou vídeos para que àqueles outros não sejam divulgados, o que inicia um círculo vicioso de envio de pornografia e ameaças. Em alguns casos, sites ou blogs inteiros são alimentados por apenas uma vítima que, lamentavelmente, "caiu na conversa" e cedeu à falsa ameaça inicial dos criminosos. A falsa sensação de anonimato colabora ainda mais para a popularidade desse tipo de delito, e quanto maior a sensação de poder e controle que o criminoso exerce sobre a vítima, maior também a ideia de que tudo é permitido, e que não existem punições para este tipo de conduta."

Ao analisar como agem os atacantes no crime de sextorsão, é perceptível que podem atuar de maneira clandestina para conseguir conteúdo privado de certa pessoa, ou seja, invadem o dispositivo eletrônico e adquirem sem permissão as informações. Como, por outro lado, conseguem da própria vítima após uma falsa ideia de relacionamento amoroso e estabelecendo uma relação de

---

[173] BERNARDO, Gabriel Cabriote; PRADO, Florestan Rodrigo do**. A Pornografia de Vingança e as novas vertentes de Crimes Sexuais Cibernéticos:** uma Breve Análise Crítica**.** V. 17, n. 17 (2021, p. 05). ETIC - ENCONTRO DE INICIAÇÃO CIENTÍFICA - ISSN 21-76-8498.

confiança, por fim, na posse dos dados passam para a segunda fase que seria exigir dinheiro ou mais fotos íntimas.

Com o escopo de delinear a forma de atuação dos criminosos, Schivon[174] disserta:

> "Nella prima, le immagini possono essere il frutto di un'attività di hacking, ossia di accesso non autorizzato al sistema informatico in uso alla vittima: vengono prelevati dal computer o da altri dispositivi o servizi di cloud storage immagini o video intimi o sessualmente espliciti prodotti consensualmente e per fini propri. Non vi è, quindi, alcun precedente contatto con la vittima, che viene contattata solo una volta andato a buon fine l'accesso non consentito e ricattata con il materiale in tal modo ottenuto. Spesso, viene richiesto il pagamento in bitcoin o altra moneta virtuale per poter accedere nuovamente ai file e rientrare in possesso dei propri contenuti o per ricevere via e-mail un programma per la decriptazione."

Ainda com o objetivo de esclarecer as formas de atuação de cibercriminosos, Schiavon[175] estabelece:

> "Diversamente, può accadere che le condotte di sextortion si sviluppino secondo un processo più complesso che punta ad un maggiore coinvolgimento della vittima. Privilegiato luogo di contatto sono ovviamente gli spazi virtuali come chat o siti virtuali, per lo più legati ai servizi di online dating, bacino di possibili utenti vulnerabili, che vengono attirati, utilizzando un profilo falso, creato ad hoc, come nel caso delle romance fraud, fenomeno al quale può essere per certi aspetti accomunato. Una volta instaurato il contatto, la vittima viene adescata, quasi corteggiata, e nel tempo, lusingata dalle promesse di maggiore intimità, non necessariamente di affettività. Ciò rende il sextortion a dispetto delle romance scam un fenomeno potenzialmente più accelerato nella sua progressione. Il tema sessuale viene introdotto in maniera graduale, in modo da sensibilizzare la vittima e indurla poi a scambiare informazioni personali e immagini sessualmente esplicite o intime, le quali saranno poi oggetto della successiva condotta estorsiva. Viene richiesto il pagamento di denaro, dietro minaccia di una pubblica esposizione on line dei materiali intimi fino ad allora condivisi."

Após o conhecimento de como agem para conseguir provocar prejuízo ao patrimônio das vítimas ou, por outra face, atentar contra a liberdade sexual e

---

[174] SCHIAVON, Alessia. **Cat-Fish, Romance Fraud e Sextortion**: le nuove frontiere dell'adescamento nei social media. Informatica e diritto, XLIII annata, Vol. XXVI, 2017, n. 1-2, pp. 177-200.

[175] SCHIAVON, Alessia. **Cat-Fish, Romance Fraud e Sextortion**: le nuove frontiere dell'adescamento nei social media. Informatica e diritto, XLIII annata, Vol. XXVI, 2017, n. 1-2, pp. 177-200.

intimidade delas, resta descobrir quais são os passos necessários a serem adotados para melhor alcançar a autoria delitiva e também o que fazer para comprovar a materialidade deste crime.

Primeiramente, verificar quais são os provedores de aplicação usados pelo criminoso para ter contato com a vítima, como exemplo temos o instagram, facebook e o whatsapp. Aos três deve ser solicitado o cadastro vinculado àquele endereço eletrônico (facebook) perfil (instagram) ou número telefônico vinculado ao whatsapp. No mesmo oficio ou dentro da plataforma de segurança fornecida somente às autoridades (Juiz, Promotor e Delegado de Polícia) é importante requerer a conservação dos diálogos dos chats ou das conversas entre vítima e autor (como forma de evitar que sejam apagadas e prejudiquem a produção de provas). É imprescindível que no ofício de solicitação de cadastro, seja solicitado o telefone cadastrado naquele perfil e a conta de email informada para regaste das senhas.

As contas de e-mails existentes nos cadastros permitirá mais uma rodada de solicitação de informações, mas desta vez às empresas que administram as contas.

Vale ressaltar que quando se trata de whatsapp é primordial saber se o backup dos diálogos são compartilhados com uma conta google ou icloud da Apple. Isso porque, mesmo na eventualidade das conversas serem apagadas, havendo autorização judicial, a Apple ou a Google será obrigada a fornecer todos os dados telemáticos vinculados ao perfil de whatsapp. Assim, haverá um vasto material probatório que servirá como base para condenação do autor e, ainda, contribuíra para saber mais informações que ajudem na localização e identificação do transgressor da lei.

A resposta originada dos provedores de aplicação (Whatsapp, Facebook ou Instagram) possibilitará o desdobramento da atividade investigativa, consequentemente haverá margem para representar por medidas cautelares como: quebra de sigilo telefônico, telemático, interceptação telefônica e busca e apreensão domiciliar.

Obtendo-se o número de IP de acesso e do telefone cadastrado, através da ERB (Estação de Rádio Base) será possível descobrir de qual local o criminoso se encontra, demonstrando que a extraterritorialidade dos delitos virtuais não são sinônimos de impunidade, mas sim, um mero obstáculo a ser transposto pelos agentes policiais.

Existindo valores transferidos para alguma conta bancária. É plenamente possível, requerer informações diretas à instituição bancária a respeito dos dados cadastrais naquela conta específica, assim como através da quebra de sigilo bancário ter conhecimento do “caminho” do dinheiro, tendo a certeza se o valor foi transferido para outras contas e posteriormente sacado. As informações bancárias podem ajudar a encontrar terceiros participes no delito e mesmo permitir o pedido judicial de bloqueio de valores, permitindo depois o ressarcimento à pessoa que teve seu patrimônio lesado.

As diversas possibilidades de alcançar o infrator dependerá dos primeiros passos básicos que é o comparecimento da vítima na delegacia para realização de boletim de ocorrência, prestar depoimento e apresentar as conversas existentes com o infrator. Os dados preliminares são de suma importância para ser traçado um ponto de partida rumo procedimento investigativo a ser adotado e o posterior sucesso no deslinde da persecução penal.

As linhas de investigação que farão parte da persecução penal dependerão dos dados preliminares fornecidos pelo ofendido e das respostas advindas das solicitações administrativas. A partir daí os investigadores traçaram o melhor roteiro a ser seguido, porém nada impede que seja seguido diferentes frentes de investigação de forma simultânea.

A expertise e persistência trará êxito no final e demonstrará que não existe delito de sextorsão que não seja possível de elucidar. Todo o êxito dependerá da informação que se procura como se busca e onde se busca.

3.2.2. Estelionato Eletrônico

Em todo o mundo milhões de pessoas são expostas a uma multiplicidade de “golpes virtuais” seja navegando na web ou através dela, delinquentes digitais

aproveitam-se da vulnerabilidade daqueles que utilizam a rede mundial de computadores para os lesar financeiramente.

No Brasil, a migração do delito de estelionato para o meio cibernético, levou o Congresso Nacional a buscar uma medida legislativa para remediar a grande lacuna que existia com a tipificação dessa conduta dentro do ordenamento jurídico pátrio.

Posto isso, a lei 14.155 de 2021, trouxe a baila duas qualificadoras para o Código Penal, a primeira dentro do corpo do Art.155 a denominando de Furto Eletrônico, enquanto a segunda foi inserida no bojo do Art. 171, §2ºA[176], sendo atribuindo o seguinte texto:

> **Fraude eletrônica**
>
> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo. (Incluído pela Lei nº 14.155, de 2021)
>
> § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional. (Incluído pela Lei nº 14.155, de 2021)

Nesse sentido, preleciona o autor Barbagalo[177]:

> "A lei 14.155/21 alterou o crime de invasão de dispositivo informático, melhorando sua redação e aumentando substancialmente suas penas (art. 154-A do CP). Além disso, finalmente, foram criados os crimes específicos de furto mediante fraude eletrônica (art. 155, § 4º-B do CP) e de fraude eletrônica (art. 171, § 2º-A do CP). A mesma lei ainda definiu o local competente para julgar os crimes de estelionato cometidos por meio de cheque sem fundos, com pagamento frustrado, ou por transferência de valores que passou a ser, nesses casos, o local da residência da vítima (art. 70, § 4º, CP).

---

[176] **CÓDIGO PENAL BRASILEIRO**, https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm, acesso em 12/08/2022.

[177] BARBAGALO, Fernando Brandini. **O novo crime de fraude eletrônica e o princípio da legalidade**. Publicado em https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/artigos-discursos-e-entrevistas/artigos/2022/o-novo-crime-de-fraude-eletronica-e-o-principio-da-legalidade. Acesso em 20/12/2022.

O legislador atribuiu o termo fraude eletrônica para os prejuízos patrimoniais provocados contra terceiros através de informações fornecidas ou mesmo obtidas clandestinamente por correios eletrônicos, redes sociais ou contatos telefônicos. Além disso, também foi introduzida no corpo do artigo uma causa de aumento de pena que implica no aumento de 1/3 a 2/3 se na prática delitiva o infrator utiliza servidor mantido fora do território nacional como forma de dificultar a sua localização e identificação.

Na visão de Estefam[178] a chegada da norma:

> ".. vem em boa hora, uma vez que, nos últimos tempos, há uma sensação deletéria de que as redes sociais constituem ambiente livre ou "terra de ninguém". A impunidade que impera nos meios virtuais, incentivada por perfis falsos ou de pessoas que se escondem atrás do anonimato, exige uma resposta penal à altura da mácula provocada ao bem protegido."

Sem sombra de dúvida, o Estelionato Eletrônico é o crime cibernético mais comum entre todos catalogados como crimes digitais e também o que atinge o maior número de vítimas. Dois fatores são cruciais para que isso aconteça, o grande número de pessoas conectadas à internet exercendo uma multiplicidade de atividades, o segundo seria a variedade de ações fraudulentas por meio virtual que conseguem atingir, a todo tempo, mais e mais vítimas.

Segundo Teixeira[179]:

> "A informatização crescente das várias atividades desenvolvidas individual ou coletivamente na sociedade veio colocar novos instrumentos nas mãos dos criminosos, cujo alcance ainda não foi corretamente avaliado, pois surgem a cada dia novas modalidades de lesões aos mais variados bens e interesses que incumbe ao Estado tutelar, propiciando a formação de uma criminalidade específica da informática, cuja tendência é aumentar quantitativamente e, qualitativamente, aperfeiçoar os seus métodos de execução"

Nos dias atuais, as tentativas de ludibriar as pessoas para obter delas informações preciosas como senhas, transferência de valores em dinheiro,

---

[178] ESTEFAN, André. **Direito Penal**: Parte Especial – Arts. 121 a 234-C – v. 2. São Paulo : SaraivaJur, 2022, p.650.
[179] TEIXEIRA, T. **Direito Digital e Processo Eletrônico**. 1 ed. São Paulo: Editora Saraiva, 2020, p. 214.

permissão para acesso a contas bancárias são difundidas de diversas formas, seja por torpedo, correio eletrônico, mensagem em rede social ou em aplicativos como whatsapp, por trás da engenharia social aplicada o desejo do delinquente virtual é sempre o mesmo, obter lucro indevido e causar significativos prejuízos.

De forma bem didática os autores Wendt e Jorge[180] lecionam que a engenharia social "é a utilização de um conjunto de técnicas destinadas a ludibriar a vítima, de forma que ela acredite nas informações prestadas e se convença a fornecer dados pessoais nos quais o criminoso tenha interesse ou a executar alguma tarefa e/ou aplicativo".

De acordo com Pereira[181]:

> "A maioria desses golpes funciona porque as vítimas acreditam que se trata de algo verdadeiro e, então, entregam aos criminosos suas informações com mais facilidade. O principal objetivo do criminoso, nesse caso, é convencer a vítima a entregar suas informações voluntariamente em vez de usar ameaças ou intimidação forçada"

O estelionato tornou-se então muito popular e a todo tempo se sabe de uma nova estratagema usada para proveito criminoso, tanto nos programas de TV ou na roda de amigos, difícil não conhecer alguém que não tenha alguma vez acessado um site falso de uma loja ou banco, ou ainda pago um boleto bancário fraudulento achando que era autêntico.

Posto isso, as autoras Lorenzo e Scaravelli[182] afirmam que esse tipo de crime contra o patrimônio possui algumas características

> "Qualquer conduta ilegal, não ética, ou não autorizada que envolva o processamento automático de dados e/ou transmissão de dados. Essa criminalidade apresenta algumas características, entre elas: transnacionalidade (veiculada virtualmente, todos os países têm acesso e fazem o uso da informação), universalidade (é um fenômeno de massa e não de elite) e ubiquidade (está presente nos setores privados e públicos)."

---

[180] WENDT, Emerson; JORGE, N.V.H, **Crimes cibernéticos, ameaças e procedimentos de investigação**. 2ª ed. Rio de Janeiro: Brasport, 2013, p.21.

[181] PEREIRA, Deocley Pedrada. **Crimes cibernéticos**: pequenos passos na prevenção de fraudes por meio de dispositivos móveis. 2021, p.18.

[182] LORENZO, Larissa Papandreus; SCARAVELLI, Gabriela Piva. **Cibercrimes e a Legislação Brasileira**, 2021, p.54. Disponível em https://dir.fag.edu.br/index.php/direito/article/view/83. Acesso em : 02 de Janeiro de 2023.

O ponto fulcral para o deslinde da persecução penal nesses casos é seguir o “caminho” do dinheiro, pois como é um delito patrimonial, ao final sempre a quantia da pessoa prejudicada vai parar em uma ou várias contas bancárias do autor ou de pessoas ligadas a ele, popurlamente chamado de “laranjas”. Ao mesmo tempo, pedir os cadastros das instituições bancárias, operadores de telefonia, sites, provedores de aplicação como instagram, facebook, whatsapp. Por todos os lados deve-se cercar o criminoso que quase sempre deixa uma brecha para se chegar até ele.

Dificilmente, após todas essas ações e a obtenção de uma gama variada de dados, o infrator conseguirá ainda manter-se no anonimato. Uma vez que se tenha conhecimento do nome verdadeiro do autor, haverá possibilidade do desdobramento das investigações e com isso, novas demandas judiciais poderão ser requeridas. Desta vez, ocorrerá a representação de busca e apreensão domiciliar, para obtenção de mais provas e apreensão do meio para prática do delitos (computador ou telefone celular), caso haja, previsão legal, também se pleiteia a restrição da liberdade do autor através de prisão preventiva ou temporária.

Diante das possibilidades aqui ventiladas, nota-se que com certo conhecimento técnico e o comprometimento de coibir esses tipos delitivos, é plenamente viável o emprego de situações que desencadeiem na definição da autoria e coleta de dados que consistam na comprovação da existência do crime.

3.2.3. Crimes contra honra e o uso dos falsos perfis

O ambiente virtual permitiu um livre espaço para que pessoas possam se manifestar e tecer opinião sobre diversas temáticas. Não importa se o assunto gire em torno de religião, esporte ou política, tornou-se um campo democrático onde toda e qualquer pessoa pode manifestar o seu comentário.

O grande problema gira em torno dos limites e regramentos desse espaço, alguns aproveitam o não contato pessoal para escrever coisas que talvez pessoalmente jamais explanaria. Além disso, equivocadamente existem aqueles que pensam que este ambiente é livre e sem regras para poder dizer o que bem entender. Nesse momento, o individuo avança do lado legal para o âmbito da

criminalidade, pois tecer comentários difamatórios, Art. 139 do Código Penal, utilizar de dizeres discriminatórios (injúria racial ou racismo), ofender a honra subjetiva de pessoas com palavrões (Injúria), Art. 140 do CP e fazer apologia, Art. 287 do CP, ou incitar, Art. 286 do CP à prática de delitos, todos, são condutas típicas dentro do Código Penal ou em legislação especial, como é o caso do Racismo.

Enquanto o transgressor mantiver o seu perfil nas redes sociais dentro da normalidade, não haverá problema para a vítima identificar o oponente e informar para a polícia.

O verdadeiro dilema encontra-se no uso de perfis falsos no twitter, instagram, salas de bate papo ou facebook sobre o qual o criminoso visa esconder sua identidade real e trazer todo o tipo de prejuízo para terceiros.

Da mesma forma, quem utiliza número de telefone com cadastro diverso e participa de grupos no Telegram ou Whatsapp , aproveitando-se do anonimato para agir criminosamente.

No ponto de vista prático, como melhor proceder no campo da investigação para que se possa chegar naquele que busca omitir sua real identidade e continuar no ramo da delinquência.

O primeiro passo é registrar a ocorrência e reduzir a termo as informações repassadas pela pessoa ofendida. Ato contínuo preservar as primeiras provas, conversas ou postagens apresentadas pela vítima. Nesse último caso, a preservação pode ser realizada por intermédio de uma ata notorial em cartório, ou mesmo pelo atestado de fé pública conferido pelo escrivão de polícia, analisando as informações e conferindo a veracidade com aquilo que foi postado.

Necessário se faz destacar a observação traçada por Távora[183] a respeito da valoração de um documento eletrônico, “deve-se aferir sua autenticidade e produzi-lo de forma lícita. Nem sempre é possível constatação da autoria, como nos casos de mensagens de correio eletrônico ou whatsapp de procedência desconhecida”.

---

[183] TÁVORA, Nestor; ALENCAR, Rosmar Rodrigues. **Novo Curso de direito processual penal**. Salvador: JusPODIVM, 2020, p.911.

Ainda tecendo considerações sobre produção de prova documental nos crimes virtuais, Zaniolo[184] estabelece que “não resta dúvida da dificuldade de obtenção de prova documental, pois o tráfego de informações nos crimes modernos é eminentemente digital: tais arquivos são facilmente adulteráveis”.

O passo seguinte a ser dado é ir em busca dos dados cadastrais perante o Facebook, Twitter, Instagram, Telegram ou Whatsapp, além de requisitar que as mensagens originadas daquele perfil investigado sejam preservadas. Alguns dados são de suma importância como: nome e informações pessoais do usuário, telefone de cadastro, email de cadastro, email de recuperação de conta, números de IP de acessos e Localização Geográfica de onde acessa.

Algumas informações secundárias podem ser requeridas administrativamente, após se ter o conhecimento da conta de email de cadastro e a de resgate da senha. Logo, é possível solicitar dos provedores de aplicação os dados cadastrais vinculados a cada conta de email.

A partir das respostas se iniciará a segunda fase que implica em uma demanda judicial, em virtude da necessidade de informações protegidas por lei e também pela tutela dos princípios constitucionais da privacidade, intimidade e não violação das comunicações telefônicas. Direcionado ao Poder Judiciário deverá ser enviado pedido solicitando autorização para quebra de sigilo telemático (conversas e mensagens armazenadas nos provedores de aplicação), a quebra de sigilo telefônico com o histórico de ligações, acessos à internet, Ips de acesso e Localização Geográfica.

A tarefa árdua para conseguir definir o verdadeiro nome do investigado será recompensada com a obtenção do endereço e dos dados pessoais dele. Por conseguinte, uma vez identificado, notifica o envolvido para interrogatório e conclui exitosamente o procedimento o encaminhando, ao final, para o Poder Judiciário.

3.2.4. Revenge Porn

As relações sociais modernas passam pela intervenção, muitas vezes de forma natural, de meios eletrônicos e da tecnologia. A cultura do sexting (troca de

[184] ZANIOLO, Pedro Augusto. **Crimes Modernos**: Os impactos da Tecnologia no Direito. Salvador: Editora JusPodium, 2021, p.50.

fotos sensuais e mensagens por aplicativos dos smartphones) se popularizou entre os casais e como demonstração de intimidade e confiança tornou-se algo extremamente comum.

Zaniolo[185] leciona que sexting é o fenômeno de "fotografar ou filmar a si próprio em momento de intimidade e transmitir as imagens por celular que nasceu nos Estados Unidos, onde é chamado de sexting – neologismo que une sex (sexo) e texting (troca de mensagens pelo smartphone)".

O fetichismo de tirar fotografias e filmar atos sexuais ou poses eróticas migrou do mero exibicionismo para uma situação de autoafirmação. A necessidade de recordar a performance intimista do casal se popularizou e depois de um certo tempo virou caso de polícia.

Buscando definir o chamado pornô de vingança, Bernardo e Prado[186] lecionam:

> "Conhecida internacionalmente como "Revenge Porn" consiste na conduta delituosa de divulgação de imagens íntimas – contendo cenas de sexo, ou não – sem autorização, de uma ou mais pessoas, e possui na grande maioria das vezes o condão de exposição e vingança em relação às vítimas que, quando se dão conta, têm fotos e vídeos íntimos espalhados por toda a web. O tema se torna ainda mais delicado quando as fotos e vídeos são produzidos pela própria vítima (fato que vem ganhando cada vez mais popularidade entre jovens e adultos, haja vista a crescente tendência à auto exposição e auto filmagens decorrente da popularização das redes sociais – hoje em dia tudo é fotografado, filmado e divulgado), que geralmente fornece o conteúdo ao parceiro ou parceira, como forma de intimidade entre o casal, mas que depois se transforma em moeda de troca – ou até uma arma nas mãos de quem pretende causar dano ao companheiro."

No revenge porn a vítima em potencial é a mulher que nesse caso não tem muitas dúvidas de quem seria o propagador das suas fotos ou vídeos sensuais. Muitas ocasiões o marido, namorado ou companheiro não aceita o término do relacionamento e por vingança com objetivo de denegrir a imagem da ofendida, propaga o conteúdo pela rede social, grupos de aplicativos (por exemplo: telegram e

---

[185] ZANIOLO, Pedro Augusto. **Crimes Modernos**: Os impactos da Tecnologia no Direito. Salvador: Editora JusPodium, 2021, p.525.

[186] BERNARDO, Gabriel Cabriote; PRADO, Florestan Rodrigo do. **A Pornografia de Vingança e as novas vertentes de Crimes Sexuais Cibernéticos**: Uma Breve Análise Crítica. V. 17, n. 17 (2021). ETIC - ENCONTRO DE INICIAÇÃO CIENTÍFICA - ISSN 21-76-8498, p.9/10

whatsapp) ou em sites de conteúdo adulto. Do ato de vingança contra a pessoa prejudicada que derivou o nome de revenge porn (pornô de vingança).

Nessa mesma toada, Bernado e Prado[187] denotam que:

> "A grande maioria das vítimas são mulheres, em grande parte jovens, que, após o término de namoros ou relacionamentos informais de curto prazo, são postadas em nas redes sociais e sites de conteúdo sexual/adulto para mero entretenimento da indústria pornográfica – cena triste e comum nos dias atuais. Cabe ainda ressaltar que a conduta de divulgação de cena íntima/sexual, sua distribuição, publicação ou oferecimento, por qualquer meio – constante no Código Penal através do artigo 218-C..."

Caletti[188] discorre a conduta delituosa como uma nova tendência cultural e social, na sua concepção:

> "Il "revenge porn" costituisce senz'altro un problema della nostra epoca. L'incidenza statistica considerata lascia in proposito ben pochi dubbi: alimentato dal "sexting" e, più in generale, dall'ingresso delle tecnologie nelle relazioni sentimentali, il fenomeno si sta diffondendo rapidamente e i dati americani lasciano presagire, nel prossimo futuro, un ulteriore incremento dei casi anche nel contesto europeo. Del resto, come si è rilevato, l'affermarsi della "revenge pornography" nasconde dietro di sé la radicalizzazione di nuove tendenze sociali e culturali."

A conduta ora abordada implica nos crimes contra a honra de difamação e injúria, como também poderá caracterizar falsa identidade (na eventualidade do propagador usar um perfil falso), além do delito principal situado no Art. 218C de publicar, divulgar ou transmitir sem o consentimento da vítima cena de nudez, pornografia ou sexo.

Nitidamente, preocupado com o crescente volume dessa ação criminosa que até 2018 não detinha uma punição específica, ficando o autor sendo responsabilizado somente pelos delitos contra a honra. Desta forma, visando preencher essa lacuna legislativa, no bojo do código penal foi acrescentado o artigo 218C que faz a alusão a essas e outras condutas. Entretanto, para sacramentar

---

[187] BERNARDO, Gabriel Cabriote; PRADO, Florestan Rodrigo do**. A Pornografia de Vingança e as novas vertentes de Crimes Sexuais Cibernéticos:** Uma Breve Análise Crítica. V. 17, n. 17 (2021). ETIC - ENCONTRO DE INICIAÇÃO CIENTÍFICA - ISSN 21-76-8498, p.10.

[188] CALETTI, Gian Marco. Revenge porn e tutela Penale. Diritto Penale Conteporaneo. Rivista Trimestrale. V3. 2018, p.100.

qualquer dúvida, restou previsto uma causa de aumento no parágrafo primeiro exasperando a pena do propagador do conteúdo que age com fim de cometer vingança, *in verbis:*

> Art. 218-C. Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio - inclusive por meio de comunicação de massa ou sistema de informática ou telemática -, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia: (Incluído pela Lei nº 13.718, de 2018)
>
> Pena - reclusão, de 1 (um) a 5 (cinco) anos, se o fato não constitui crime mais grave. (Incluído pela Lei nº 13.718, de 2018)
>
> Aumento de pena
>
> **§ 1º A pena é aumentada de 1/3 (um terço) a 2/3 (dois terços) se o crime é praticado por agente que mantém ou tenha mantido relação íntima de afeto com a vítima ou com o fim de vingança ou humilhação**. (Incluído pela Lei nº 13.718, de 2018).

Portanto, como se pode observar em texto citado, a lei 13.718 de 2018, trouxa a baila a previsão como crime de comportamento que se tornou usual e, de certa forma, cultural o de utilizar desse mecanismo para denegrir a imagem, principalmente, das mulheres no âmbito da sociedade.

Compete às polícias judiciárias agirem para preservar o direito das ofendidas, tendo como principal tarefa identificar o criminoso, se desconhecido, preservar as provas e buscar retirar o conteúdo dos locais onde estão hospedados.

Importante ressaltar que todas aquelas pessoas que repostam essas imagens ou vídeos respondem de mesma forma do que aquele que for identificado como a primeira pessoa que divulgou.

Na eventualidade do material constar em um site de conteúdo adulto, o caminho inicial é registrar a prova e comprovar a sua autenticidade, ato contínuo solicitar ao administrador do portal o cadastro com todos os dados do indivíduo que disponibilizou aquele conteúdo no site da web. Em seguida, deverá ser solicitado ao administrador que retire o conteúdo da sua página apresentando cópia do boletim de ocorrência, sob pena de responder também pelo delito em comento.

Não se pode olvidar que hackers podem invadir o dispositivo eletrônico e tendo acesso ao conteúdo ilicitamente disponibilizam em sites ou grupos de whatsapp ou telegram para acesso de milhares de pessoas.

No que tange ao material constar em grupos de bate papo e troca de fotos e vídeos, os agentes devem solicitar a preservação dos dados que constam naquele determinado grupo, depois o cadastro de todos os participantes, bem como o acesso ao conteúdo. Dessa forma, identificará o primeiro a ter disponibilizado o material proibido, assim saberá e identificará os demais envolvidos.

Enfim, a complexidade delitiva é notória, mas a impunidade não poderá prosperar. Enquanto os vídeos e fotos da ofendida estiverem circulando na web, as ações delitivas persistirão e só com a responsabilização dos propagadores é que didaticamente o Revenge Porn sairá do ambiente cultural da sociedade moderna.

CONSIDERAÇÕES FINAIS

A atividade de polícia investigativa no Brasil passa por um importante período de transição, ao qual o dinamismo dos fatos delituosos obriga uma urgente adaptação e atualização dos procedimentos e técnicas investigativas.

A era digital gerou para o período pós-moderno um impacto significativo que altera a forma de vida de todas as pessoas dentro do mesmo meio social. Essa revolução tecnológica tornou todos um pouco dependentes dos novos dispositivos tecnológicos que foram muito além de ser um mero instrumento de trabalho, tornando-se um elemento primordial que passa a fazer parte na vida dos indivíduos.

Os avanços trazidos pelo novo período também apresenta um moderno catálogo de delitos, uma vez que inúmeras atividades de pessoas físicas e jurídicas são executadas por intermédio da internet. Essa nova gama de crimes cometidos por intermédio da internet é denominada de delitos cibernéticos, sendo que alguns são considerados tipicamente virtuais, crimes cibernéticos próprios, já outros são os crimes comuns que passam ser cometidos também pela internet, recebendo a nomenclatura de crimes virtuais impróprios.

No ambiente virtual surgiu um novo tipo de delinquente com uma nova categoria de infração penal, tudo muito recente para os agentes da investigação. Dia após dia as vítimas buscam as delegacias de todo país para noticiar um fato delituoso dessa seara, obrigando uma mudança desde o atendimento até os procedimentos a serem adotados.

O presente trabalho destacou que a lesão aos bens jurídicos nos crimes digitais vão muito além daquilo que se encontra à primeira vista, pois atinge a raiz de todo o direito inerente ao ser humano que é a sua dignidade. Direito constitucional elencado na Carta Magna brasileira.

Mesmo que as infrações penais digital violem direitos como patrimônio, liberdade sexual e honra, sempre terá como cerne de proteção a dignidade da pessoa humana, princípio e fundamento da República Federativa do Brasil.

Diante disso, o cenário atual provoca os congressistas a legislarem a favor da criação de novas leis, como a Lei Geral de Proteção de Dados e o Marco Civil da Internet, assim como a adequação no próprio corpo do Código Penal e em

algumas leis especiais, abarcando novas infrações penais, como as cometidas pela rede mundial de computadores. Todo o arcabouço legislativo serve de anteparo para coibir o contemporâneo perfil dos autores e como forma de “escudo” de proteção para a população.

A democratização do acesso à internet e o desenvolvimento da tecnologia elevou o usuário a uma posição de extrema vulnerabilidade. Obstáculos como a extraterritorialidade dos ilícitos virtuais e a carência de mecanismos eficazes no seu combate elevou o número de crimes e de vítimas.

As policiais investigativas de todo o país precisam encontrar técnicas investigativas para lidar com a mutação dos crimes tradicionais para delitos virtuais, como o estelionato eletrônico, sextorsão, revenge porn, criação de falsa identidade em perfis de rede social, crimes contra a honra na web, falsificações de páginas da web e documentos eletrônicos, auxílio, induzimento e instigação ao suicídio, como o chamado “baleia azul”, que atingem o público infanto-juvenil.

Por outro lado, investigadores são pegos de surpresa com delitos virtuais próprios como o dano informático, invasão de dispositivo eletrônico, interceptação clandestina de dados informáticos e telemáticos e a inserção fraudulenta de vírus e malwares com o fim de causar prejuízo. Surgindo como desafio o conhecimento técnico e específico para enfrentar a demanda.

A multiplicação de malwares como spyware, ransonware, worm e trojans trazem para o cenário policial um novo e intrigante vocabulário que requer conhecimento especial para lidar com tais programas maliciosos que provocam prejuízos não só materiais, mas também na função de ferramentas para cometimento de diferentes delitos de internet.

Some-se a isso, a pandemia provocada pelo Coronavírus, que em 2019 atingiu de forma acachapante todo o globo terrestre e obrigou à todos um isolamento social como forma preventiva à propagação da Covid 19. O isolamento forçado elevou o número de usuários à rede mundial de computadores e permitiu a migração de uma diversidade de serviços para o ambiente virtual. Na medida em que as pessoas passaram a utilizar esse ambiente para exercer suas atividades,

delinquentes virtuais adaptaram antigas infrações e cometeram outras ainda desconhecidas do público em geral.

A multiplicidade e numerosidade dos crimes digitais contribuíram para a criação de Delegacias Especializadas no combate a estas infrações em todos os estados da federação. Porém, o crescimento exponencial das ofensas aos bens jurídicos na internet, transpareceu a limitação da Administração Pública na proteção desses direitos.

Fatores como a extraterritorialidade dos crimes virtuais, a falta de conhecimento técnico especializado, a inexistência de atendimento e procedimento especializado, bem como a falta e estrutura tornam o enfretamento ainda mais difícil.

Os desafios aqui apontados, juntamente com a transnacionalidade deste delito e sua propagação em massa, principalmente durante a pandemia, fez surgir o seguinte problema direcionado aos gestores do Poder Público que a presente dissertação busca responder: Será de fato que os agentes de polícia judiciária estão preparados para enfrentar a onda dos cibercrimes que vitimizam uma grande parcela da população e impõem desafios ao Estado e seus agentes?

O objetivo geral da pesquisa foi analisar os delitos catalogados como virtuais e sua ofensa a bem jurídicos, propondo técnicas de investigação e apontando os desafios gerais para as polícias judiciárias.

Os objetivos específicos foram: discorrer, classificar e caracterizar os delitos de internet dentro do ordenamento jurídico pátrio, sua forma de enfrentamento e quais melhores técnicas existentes para definir a autoria e comprovar a existência daqueles crimes virtuais mais habituais.

Para esta pesquisa foi levantada a seguinte hipótese: analisado as espécies de crimes digitais próprios e impróprios, especificamente, na violação dos distintos bens jurídicos, verifica-se que o aprimoramento de técnicas investigativas no âmbito da atuação investigativa, contribuirá para uma padronização de procedimento e uma uniformização das boas práticas servindo de uma poderosa frente no combate a essa espécie de delito.

O presente trabalho buscou demonstrar muito além dos desafios existentes aos agentes de polícia judiciária. Tentou estabelecer técnicas e procedimentos a serem adotados para identificar a autoria e provar a materialidade dos crimes de internet mais comuns no dia dia.

Determinadas ações se disseminadas entre os investigadores servirá de “soldado de reserva” e os capacitará apontando o caminho a ser seguido para desenvolver a persecução penal com relevância e, ao final, a consequente prisão dos criminosos virtuais.

De alguma forma, se espera colaborar com a atividade investigativa e mostrar que mesmo com a complexidade para enfrentar a nova modalidade delitiva, não é impossível identificar e prender infratores, prevenindo novos crimes e resgatando, principalmente, os direitos dos cidadãos e a sua dignidade.

REFERÊNCIA DAS FONTES CITADAS

ARAGÃO, David Farias de. **Limites constitucionais e efetividade da investigação criminal de delitos cibernéticos**. IN Combate ao Crime Cibernético. Mallet: Rio de Janeiro, 2016, p. 225.

ASCENÇÃO, J. O. **A dignidade da Pessoa e o Fundamento dos Direitos Humanos**. Revista da Faculdade de Direito da Universidade de São Paulo, v.103, 2008. Disponível em: https: //www.revistas.usp.br/rfdusp/article/views/67806. Acesso em 10.07.2022.

ASCENÇÃO, J. O. **A dignidade da Pessoa e o Fundamento dos Direitos Humanos**. Revista da Faculdade de Direito da Universidade de São Paulo, v.103, 2008. Disponível em: https: //www.revistas.usp.br/rfdusp/article/views/67806. Acesso em 10.07.2022.

BARBAGALO, Fernando Brandini. **O novo crime de fraude eletrônica e o princípio da legalidade**. Publicado em https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/artigos-discursos-e-entrevistas/artigos/2022/o-novo-crime-de-fraude-eletronica-e-o-principio-da-legalidade. Acesso em 20/12/2022.

BARRETO, Alessandro Gonçalves/Brasil, Beatriz Silveira. **Investigação Cibernética,** à luz do Marco Civil da Internet. Rio de janeiro. Brasport, 2016.

BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira. Manual **de Investigação Cibernética: à luz do Marco Civil da Internet.** Rio de Janeiro: Brasport, 2016, p. 11.

BARRETTO, Rafael. **Direitos Humanos**. Juspodium: Salvador, 2022

BARROS, Francisco Dirceu. **Tratado doutrinário de direito penal**. Salvador: Juspodium, 2018, p. 1.540.

BASTOS, Celso Ribeiro; MARTINS, Ives Gandra da Silva. **Comentários à Constituição do Brasil**. São Paulo: Saraiva, 1989, v. 2, p. 63.

BERGMANN,Pablo Barcellos. **Aspectos Penais do Marco Civil da Internet**. IN Combate ao Crime Cibernético. Mallet: Rio de Janeiro, 2016, p. 46/47.

BERNARDO, Gabriel Cabriote; PRADO, Florestan Rodrigo do**. A Pornografia de Vingança e as novas vertentes de Crimes Sexuais Cibernéticos:** uma Breve Análise Crítica**.** V. 17, n. 17 (2021, p. 05). ETIC - ENCONTRO DE INICIAÇÃO CIENTÍFICA - ISSN 21-76-8498.

BEZERRA, Clayson da Silva/Agnoletto, Giovani Celso. **Combate ao Crime Cibernético.** Rio de Janeiro. Mallet Editora, 2016, p. 117.

CALETTI, Gian Marco. Revenge porn e tutela Penale. Diritto Penale Conteporaneo. Rivista Trimestrale. V3. 2018, p.100.

CANHAS, Hermes. **Garantismo Constitucional quanto à Lei de Proteção de Dados (LGPD) e Pec 17/2019**: influências, impactos e desenvolvimento da Proteção de Dados. www.hermescanhas.jusbrasil.com.br. Acesso em 10 de Setembro de 2022.

CARDOSO, Nágila Magalhães. **A Pandemia do Cibercrime**. Porto Alegre, 2020, p. 19. Disponível em https://www.direitoeti.emnuvens.com.br/direitoeti/article/view/88/86 acessado em 15 de Novembro de 2020.

CARTILHA de segurança da internet. **Comitê Gestor da Internet no Brasil**, jun. 2012. Disponível em: https://cartilha.cert.br/lvro/cartilha-seguranca-internet.pdf>. Acesso em: 03 de Janeiro de 2023.

CASSANTI, Moisés de Oliveira. **Crimes Virtuais – vítimas reais.** Rio de Janeiro. Brasport, 2014.

CASTRO, Inês Maria Vaz Prego de**. O contributo da Polícia Judiciária na Investigação Criminal e a Cooperação Policial.** Mestrado Forense. Lisboa, 2016, p. 10.

CÓDIGO PENAL BRASILEIRO, https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm, acesso em 17/12/2022.

COMPARATO, Fábio Konder. **Fundamento dos Direitos Humanos**. Revista O tempo em Movimento, edição 36, nº 3, 2017.

Constituição Federal Brasileira, http://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm, acesso em 16 de Setembro de 2022.

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

CRUZ, Paulo/Stelzer, Joana. **Direito e Transnacionalidade.** Curitiba. Editora Juruá, 2009, p. 134.

CUNHA, Rogério Sanches. **Lei 14.155/21 e os crimes de fraude digital. Primeiras impressões e reflexos no CP e no CPP**. In https://meusitejuridico.editorajuspodivm.com.br/2021/05/28/lei-14-15521-e-os-crimesdefraude-digital-primeiras-impressoes-e-reflexos-no-cp-e-no-cpp/.(2021) Acessado 18 de 0utubro de 2022.

D'URSO, Adriana Filizzola, **Sextorsão e Estupro Virtual:** Novos Crimes Na Internet. São Paulo,2017, p. 01. http://www.cjlp.org/materias/ARTIGO%20%20Sextorsao%20e%20Estupro%20Virtual_Adriana_Filizzola_DUrso.pdf. Acesso em 06 de Dezembro de 2022.

DA SILVA, Edson Ferreira. **Direito à Intimidade**. São Paulo: Ed. Oliveira Mendes, 1998, p. 39.

DARÓS MALAQUIAS, Roberto Antônio. **Crime Cibernético e Prova,** investigação criminal em busca da verdade. Curitiba. Editora Juruá, 2015, p.38

DE CUPIS, Adriano. **Os Direitos de Personalidade**. São Paulo: Ed. Romana,2004, p. 283.

ESTEFAN, André. **Direito Penal**: Parte Especial – Arts. 121 a 234-C – v. 2. São Paulo : SaraivaJur, 2022.

FALCÃO JUNIOR, Alfredo Carlos G./ Buffon, Jaueline Ana. **Crimes Cibernéticos**: Racismo, Cyberbullying, Deep Web, Pedofilia e Pornografia Infanto Juvenil, Infiltração de Agentes por Meio Virtual, Obtenção das Provas Digitais e Nova Lei Antiterrorismo. Porto Alegre. Livraria do Advogado, 2017.

FERREIRA, Lúcia de Fátima Guerra; ZENAIDE, Maria de Nazaré Tavares; NÁDER, Alexandre Antônio Gili; **Educando em Direitos Humanos**: fundamentos histórico-filosófico e políticos jurídicos. Editora da UFPB: João Pessoa, 2016.

FIORILLO, Celso Antônio Pacheco. **O Marco Civil da Internet e o Meio Ambiente Virtual na Sociedade da Informação**: Comentários à Lei 12.965/2014, (2015, P.5/6).

FRAGOSO. Henleno Cláudio. **Lições de direito penal**: Parte Especial. 11ed. Atualiz. Por Fernando Fragoso. Rio de Janeiro: Forense, (2005, P.277).

FURLANETO NETO, Mário; SANTOS, José Eduardo Lourenço dos; GIMENES, Eron Veríssimo. **Crimes na internet e inquérito policial eletrônico**. São Paulo: Edipro, 2012.

GARCIA, Lara Rocha. **Lei Geral de Proteção de Dados Pessoais (LGPD):** Guia de implantação/ Lara Rocha Garcia; Edson Aguilera Fernandes; Rafael Augusto Moreno Gonçalves; Marcos Ribeiro Pereira-Barretto. São Paulo: Bluchen, 2020, p. 17.

GOMES, Luiz Flávio; CERVINI, Raúl. **Interceptação telefônica**. São Paulo: RT, 1997, p.71.

GRECCO, Rogério. **Curso de Direito Penal**: parte especial, volume III. Niterói: Impetus, (2015).

GRECCO, Rogério. **Curso de Direito Penal**: parte especial, volume III. Niterói: Impetus, (2015, P.237).
https://pt.wikipedia.org/wiki/Coronavírus, acesso dia 29 de Novembro de 2021

HUNGRIA, Nélson. **Comentários ao código penal**. São Paulo: Forense, (2007, P.308).

JESUS**,** Damásio Evangelista de. **Interceptação de comunicações telefônicas**: notas à Lei nº 9.296, de 24.07.1996. Revista dos Tribunais, São Paulo, 1997.

Lei de Interceptação Telefônica, 9296/1996. https://www.planalto.gov.br/ccivil_03/leis/l9296.htm. Acesso em 03 de Janeiro de 2023.

LEI GERAL DE PROTEÇÃO DE DADOS, lei 13.709/18, http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 01/10/2022.

LORENZO, Larissa Papandreus; SCARAVELLI, Gabriela Piva. **Cibercrimes e a Legislação Brasileira**, 2021, p.54. Disponível em https://dir.fag.edu.br/index.php/direito/article/view/83. Acesso em : 02 de Janeiro de 2023.

LORUSSO, Piero. **L'insecurezza dell'era digitale**: Tra cybercrimes e nuove fronteire dell'investigazione. Confini Sociologici. Franco Angeli. Milano, 2011, p. 08.

Marco Civil da Internet. Acesso realizado em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

MASSON, Cleber. **Direito Penal Esquematizado, vol.3: parte especial**. Método: São Paulo, 2013.

MENDES, Laura Schertel; DONEDA, Danilo. **Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados**. Revista de Direito do Consumidor, São Paulo, v. 120, ano 27, p. 469- 483, nov./dez. 2018. Disponível em: https://revistadedireitodoconsumidor.emnuvens.com.br/rdc/article/view/1116. Acesso em: 10 jul. 2022.

MIRAGEM, Bruno. **A Lei Geral de Proteção de Dados (Lei 13.704/2018) e o direito do Consumidor**. Revistas dos Tribunais. Vol. 1009/2019. Nov/2019, p. 02.

MONTEIRO, Renato Leite. **Existe um direito à explicação na Lei Geral de Proteção de Dados no Brasil?** Instituto Igarapé. Artigo Estratégico nº 39. Dezembro de 2018.

MORAES, Alexandre de. **Direitos Humanos Fundamentais** - Teoria Geral. São Paulo: Atlas. (2011, p. 240).

MORAES, Alexandre de. **Direitos humanos fundamentais**: comentários aos arts. 1º ao 5º da Constituição da República Federativa do Brasil. São Paulo: Atlas, 1997, v. 3, p. 39.

NORONHA, Magalhães. **Direito Penal**: crimes contra a pessoa e crimes contra o patrimônio. São Paulo, 1973.

PALFREY, John. GASSER, Urs. **Nascidos na Era Digital** – Entendendo a Primeira Geração de Nativos Digitais. Ed Artmed. Porto Alegre, 2011.

PEREIRA, Deocley Pedrada. **Crimes cibernéticos**: pequenos passos na prevenção de fraudes por meio de dispositivos móveis. 2021, p.18.

PEREZ LUÑO, Antonio Henrique. **Derechos Humanos, estado de derecho y constitucíon**. Madrid: Tecno, 2003.

PULIDO, Carlos Bernal**. El principio de proporcionalidad y los derechos fundamentales.** 4. ed. Bogotá: Universidad Externado de Colombia, 2014, p. 173.

ROSENDO Juliana Vital; CARVALHO Grasielle Borges Vieira de; **Os novos desafios e perspectivas acerca da investigação criminal no Brasil.** Cadernos de Graduação. Aracaju, 2015, p. 73.

SARLET, Ingo Wolfang. **Dignidade (da Pessoa) Humana e Direitos Fundamentais na Constituição de 1988**. Porto Alegre: Livraria do Advogado Editora, 2015.

SARLET, Ingo Wolfgang. **A EC115/22 e a proteção dos dados pessoais como Direito Fundamental**. www.conjur.com.br. Acesso em 12 de Setembro de 2022.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**. 7. ed. Porto Alegre: Livraria do Advogado, 2007, p. 177.

SCHIAVON, Alessia. **Cat-Fish, Romance Fraud e Sextortion**: le nuove frontiere dell'adescamento nei social media. Informatica e diritto, XLIII annata, Vol. XXVI, 2017, n. 1-2, pp. 177-200.

SILVA FILHO, Acácio Miranda da ... [et al.]; coordenadores Mauricio Schaun Jalil, Vicente Greco Filho. **Código Penal comentado**: doutrina e jurisprudência. Barueri [SP]: Manole, 2020.

SILVA, Elizabet Leal da. ZENI, Alessandro Severino Vallér. **Algumas considerações sobre o Princípio da Dignidade da Pessoa Humana**. Revista Jurídica Cesumar – Mestrado, v.9, n.1, jan/jun 2009 – ISSN1677-6402.

SILVA, José Afonso da. **A dignidade da Pessoa Humana como valor supremo da democracia**. Revista do Direito Administrativo. nº212, abr/jun. Rio de Janeiro, 1998.

SILVA, Marco Antônio Marques da. **Acesso à justiça penal e estado democrático de direito**. São Paulo: Juarez de Oliveira, 2001.

SILVEIRA, Maria Ana Barroso de Moura da. **Da problemática da Investigação Criminal em Ambiente Digital** - em especial, Sobre a Possibilidade de utilização de malware como meio oculto de obtenção de prova. Mestrado Forense, Lisboa, 2016, p. 07.

SOARES, Maria Victoria de Mesquita Benevides. **Cidadania e Direitos Humanos**. Revista Cadernos de Pesquisa, vol. 45. Fundação Carlos Chagas:2014.

SOARES, Ricardo Maurício Freire. **O princípio da dignidade da pessoa humana**: em busca do direito justo. São Paulo: Saraiva, 2010.

SYDOW, Spencer Toth; CASTRO, Ana Lara Camargo. **Sextorsão.** Vol. 959. Revistas dos Tribunais, 2015, p. 01.

TÁVORA, Nestor; ALENCAR, Rosmar Rodrigues. Novo Curso de direito processual penal. Salvador: JusPODIVM, 2020, p.911.

TEFFÉ, Chiara Spadaccini de; MORAES, Maria Celina Bodin de. **Redes Sociais Virtuais**: privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet. Revistas de Ciências Jurídicas. V.22. Fortaleza: Pensar, 2017.

TEIXEIRA, T. **Direito Digital e Processo Eletrônico**. 1 ed. São Paulo: Editora Saraiva, 2020.

TUCCI, Rogério Lauria. **Direitos e garantias individuais no processo penal brasileiro**. Tese para concurso de Professor Titular de Direito Processual Penal da Faculdade de Direito da Universidade de São Paulo. São Paulo: Saraiva, 1993, p. 419.

ULBRICH, Henrique César; VALLE, James Della. **Universidade H4CK3R**. 6 ED. São Paulo: Digerati Books, 2009.

VALIN, Celso. **A questão da jurisdição e da territorialidade nos crimes praticados pela internet**. Florianópolis.: Boiteux, 2000, p. 116.

WENDT, Emerson. JORGE, Higor Vinícius Mendonça. **Crimes Cibernéticos**: Ameaças e Procedimentos de Investigação. Rio de Janeiro. Ed. Brasport, 2013.

WENDT, Emerson; JORGE, N.V.H, **Crimes cibernéticos, ameaças e procedimentos de investigação**. 2ª ed. Rio de Janeiro: Brasport, 2013, p.21.

ZANIOLO, Pedro Augusto. **Crimes Modernos**: o impacto da tecnologia no direito. Salvador: Juspodium, 2021.

ZANIOLO, Pedro Augusto. **Crimes Modernos**: Os impactos da Tecnologia no Direito. Salvador: Editora JusPodium, 2021.