PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
PRO-REITORIA DE GRADUAÇÃO
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
CURSO DE DIREITO
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO
ARTIGO CIENTÍFICO

CRIMES CIBERNÉTICOS

CRIMES CIBERNÉTICOS E SEUS IMPACTOS NA IMAGEM DO INDIVÍDUO

ORIENTANDO (A) – LUCIANA DE ALMEIDA PUPULIN NAME

ORIENTADOR (A) – NIVALDO DOS SANTOS

GOIÂNIA-GO
2023

LUCIANA DE ALMEIDA PUPULIN NAME

CRIMES CIBERNÉTICOS

CRIMES CIBERNÉTICOS E SEUS IMPACTOS NA IMAGEM DO INDIVÍDUOS

Artigo Científico apresentado à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação da Pontifícia Universidade Católica de Goiás (PUC GOIÁS).
Prof.(a) Orientador (a) – Prof. Nivaldo dos Santos.

GOIÂNIA-GO
2023

LUCIANA DE ALMEIDA PUPULIN NAME

CRIMES CIBERNÉTICOS

CRIMES CIBERNÉTICOS E SEUS IMPACTOS NA IMAGEM DO INDIVÍDUO

Data da Defesa: ____ de _____ de _____

BANCA EXAMINADORA

_____

Orientador (a): Prof. (a): **NIVALDO DOS SANTOS** Nota

_____

Examinador (a) Convidado (a): Prof. (a): **ERNESTO MARTIM S. DUNCK** Nota

CRIMES CIBERNÉTICOS

CRIMES CIBERNÉTICOS E SEUS IMPACTOS NA IMAGEM DO INDIVÍDUO

Luciana de Almeida Pupulin Name[1]

RESUMO

Este trabalho tem como objetivo realizar uma breve análise didática a respeito dos "crimes cibernéticos", explorando e sintetizando o meio do crime cibernético e os problemas que podem vir a gerar aos indivíduos, demonstrando os avanços de forma benéfica e os prejuízos que podem vir a causar quando utilizados de forma ilícita, sobretudo através da exploração de dados pessoais do individuo, com âmbito de atuação em quase todas as esferas do mundo jurídico, tendo como vítima qualquer pessoa, inclusive o próprio Estado, importante pontuar que com a finalidade de combater os delitos praticados no ambiente virtual foram promulgadas algumas leis um exemplo seria a Lei dos Crimes Cibernéticos, conhecida por Lei Carolina Dieckmann com nº 12.735 de 2012, e sobre a importância da cooperação internacional no combate, na investigação e prevenção de cibercrimes.

Palavras-chaves: Ambiente virtual. Problemas ao individuo. Direito penal brasileiro. Evolução legislativa. Crimes cibernéticos.

[1] Acadêmica do Curso de Direito da Pontifícia Universidade Católica de Goiás.

CYBER CRIMES

CYBER CRIMES AND ITS IMPACTS ON THE IMAGE OF THE INDIVIDUAL

Luciana de Almeida Pupulin Name

ABSTRACT

This paper aims to provide a brief didactic analysis on "cybercrimes", exploring and summarizing the world of cybercrime and the problems that may arise for individuals. It demonstrates the beneficial advances as well as the damages that can be caused when used illicitly, especially through the exploitation of personal data of individuals. It operates in almost all spheres of the legal world, victimizing anyone, including the State itself. It is important to note that in order to combat crimes committed in the virtual environment, some laws have been enacted, such as the Cybercrime Law, also known as the Carolina Dieckmann Law, with number 12.735 of 2012. Additionally, the paper discusses the importance of international cooperation in combating, investigating and preventing cybercrimes.

Keywords: Virtual environment. Individual problems. Brazilian criminal law. Legislative evolution. Cybercrimes.

SUMÁRIO

RESUMO ……. Pág. 03

INTRODUÇÃO ..... pág. 06

1 SEÇÃO PRIMÁRIA ..... pág. 09

Crimes cibernéticos e seus impactos.

1.1 SEÇÃO SECUNDÁRIA ..... pág. 17

Legislação especifica aplicável aos crimes digitais

1.1.1 SEÇÃO TERCIÁRIA.....pág. 27

Jurisprudência existente sobre os crimes virtuais nos tribunais brasileiros.

CONCLUSÃO .....pág. 31

REFERÊNCIAS .....pág. 33

INTRODUÇÃO

Este trabalho tem por objetivo explorar e sintetizar o meio do crime cibernético, demonstrando seus avanços e diante disso os prejuízos que podem vir a causar no meio virtual, e como não possui barreiras que limitem seu alcance de suas vítimas, podendo alcançar a pessoa em particular, as pessoas empresariais e até mesmo o próprio Estado.

Pretende-se com este trabalho analisar as particularidades e desenvolvimentos relativo aos crimes cibernéticos, demonstrando de forma a esclarecer alguns danos que podem vir a causar e até mesmo demonstrar possibilidades de se punir os infratores.

Os crimes cibernéticos surgiram conjuntamente ao avanço tecnológico ocorrido na humanidade, onde suas particularidades ficaram mais fragilizadas devido a grande quantidade de dados postados pelos usuários diariamente via virtual, seja de cunho pessoal ou financeiro trazendo consigo alguns malefícios onde ocorre a exposição das vítimas, podendo gerar alguns incômodos pessoais, sociais, financeiros, através de diversos caminhos seja por redes sociais como o Instagram, Facebook, Twitter, WhatsApp, compras via internet, ou até mesmo através de sistemas financeiros, como bancos, entre outros.

A metodologia a ser utilizada será quanto ao tipo e método, que a pesquisa se caracterize como descritiva, concernente aos meios de investigação, tratando-se de uma pesquisa bibliográfica, tendo a necessidade a análise de Leis, Decretos e demais Normas do Ordenamento Jurídico, a fim de aferir o avanço na Legislação que refere ao tema da pesquisa.

A síntese da estrutura do trabalho será:

Inicialmente de forma primaria a exposição de uma breve história de como surgiu e o desenvolvimento do uso da interne, e identificação de alguns crimes cibernéticos e seus impactos.

De forma secundaria, delimitar algumas legislações especificas aplicáveis aos crimes digitais, analisando as diversas denominações dos crimes, indicando seus principais meios, e algumas dificuldades encontradas em poder punir.

Por fim de forma terciaria expor algumas jurisprudências existente sobre os crimes virtuais nos tribunais brasileiros.

Os problemas a serem abordados são relativos a existência de diferença entre o crime cibernético, crimes digitais e crimes virtuais? e quais avanços ao qual se pode verificar de forma benéfica e prejuízos, no mundo cibernético?

Ademais, para esse estudo foi utilizado várias técnicas de pesquisa como referência, sites de busca, artigos, livros, as normas brasileiras e artigos científicos. Tendo como objetivo geral analisar os crimes cibernéticos e seus impactos na imagem dos indivíduos.

“Quanto mais a internet e os recursos tecnológicos fazem parte do nosso dia a dia, mais o princípio da intimidade se torna mitigado.

Em todo canto existem pessoas publicando fotos, vídeos ou informações sobre o que estão realizando.

A prática do chamado check-in é um exemplo disso, pois permite, inclusive, a geolocalização do indivíduo.

Considerando isso, podemos dizer que a principal forma da pessoa ter a sua privacidade respeitada é se manter longe da internet, o que poucas pessoas conseguiriam fazer nos dias atuais”

Higor Vinícius Nogueira Jorge

1 SEÇÃO PRIMÁRIA

Crimes cibernéticos e seus impactos.

O nome internet vem da origem *Internetworking,* que significa ligação entre redes, pode-se dizer que é o conjunto de todas as redes ao qual se usa a conexão como protocolo verificando entre elas linhas digitais, através de computadores, roteadores e muitas outras, sendo um conjunto físico, programas e protocolos de conexão, usados para transporte de informação, onde suas ligações podem ser chamadas de teia, ou seja onde todos estão interligados entre si, pela linha virtual.

A integração da internet mundial se iniciou de forma mais acentuada em meados da década de 70 e início dos anos 80, alterando assim a forma de comunicação entre as pessoas, onde pôde-se observar uma maior interação comercial e pessoal dos indivíduos, eles se tornaram mais inclusos ao meio virtual, sendo a internet um dos maiores avanços de comunicação da humanidade, fazendo com que o indivíduo possa obter lucros ou prejuízos.

Os primeiros crimes virtuais ocorram na década de 1960, onde se verificava atos de **sabotagem**, **espionagem** e abuso ilegal de sistemas de computadores, porém devido as condições técnicas na época não estarem atualizadas quanto o que seria esses crimes e como eles ocorriam, não se conseguia êxito em se encontrar o responsável pelo que estava ocorrendo, tinham uma dificuldade em detectar essa prática. (Agência Câmara, 2006, online)

Na década de 70 a maioria dos crimes virtuais eram praticados por especialistas em informática e geralmente se dava contra alguma instituição financeira tendo como objetivo obter a vantagem financeira. (BRIZOLA, 2016, online).

Essa modalidade de crime, conhecida como crime cibernético, até então não era muito conhecida no Brasil, passando a ter sua inclusão de forma mais acentuada apenas 30 anos após a ocorrência dos primeiros crimes cibernéticos, foi na década de 1990, sendo que em 2002 o Brasil já era considerado como o primeiro do ranking mundial na prática deste crime.

Inicialmente o tema foi tratado como uma questão de direito penal econômico, visto que a maioria dos crimes tinha como finalidade econômica, vez que no dia 18/12/1987 foi editada a Lei n.º 7.646/87, tendo como finalidade proteção à propriedade intelectual sobre programas de computador e sua comercialização no

país, sendo revogada posteriormente pelo artigo 16 da Lei nº 9.609 de 19.02.1998. (NASCIMENTO, 2016, pág. 17).

Foi a partir da promulgação da Lei 12.737 (Lei Carolina Dieckmann) datada de 30 de novembro de 2012, que o âmbito jurídico começou e ter uma visão diferenciada referente a esse novo tipo penal, dando um maior destaque a ele, se iniciou-se a identificação através de análise das características relatadas e procedimentos gerados pelos invasores, tendo uma melhor probabilidade de se ter a possibilidade de punir os infratores, foi necessário efetuar algumas alterações no Código Penal, sendo incluídos alguns artigos como 154-A, 154-B, 266 e 298.

Já ano de 2014 foi sancionada no governo de Dilma Rousseff a Lei **nº 12.965,** de 23 de abril de 2014, conhecida como “Marco Civil da Internet”, ela determinou deveres, direitos, garantias e princípios para o uso da internet no Brasil, ofereceu diretrizes para a atuação da União, dos Estados, do Distrito Federal e dos Municípios. Ela é um amparo legal relacionado aos crimes cibernéticos, tendo como recurso proteger os dados e a privacidade dos usuários na internet, além de oferecer para as vítimas que tiveram sua privacidade exposta na web poderem exigir a remoção do conteúdo.

No ano de 2018 foi publicada a Lei Geral de Proteção de Dados (LGPD) Lei 13.709/2018, em 2019 foi aprovada a PEC-17/2019 sobre proteção de dados e em 2021 através da Lei 14.132 sancionada em 31 de março de 2021 onde se inseriu no Código Penal o art. 147-A denominado como crime de perseguição (Stalking), verificando assim uma preocupação na proteção dos direitos fundamentais de liberdade e privacidade.

Desta forma a internet já não seria um ambiente livre, passando a ser monitorada por programas mais modernos, dificultando a conectividade por pessoas não autorizadas, sendo solicitadas regulamentações com o fim de se gerar uma maior proteção dos dados dos indivíduos, contudo, de forma rotineira o ambiente virtual possui uma série de armadilhas que podem comprometer o bem-estar dos usuários, sendo este um problema crescente na realidade dos brasileiros.

Para a que a prática dos crimes cibernéticos ou crimes virtuais possam ser reconhecidos o hacker[2], cracker[3] ou cibercriminosos devem fazer uso de uma rede de computadores ou de dispositivos como celulares, computadores ou tabletes, eles devem estar conectados em rede, onde na maioria das vezes o objetivo é a obtenção de lucros.

Os problemas cibernéticos podem gerar prejuízos não só no aspecto financeiro, mas também na reputação das pessoas ou empresas, os invasores costumam utilizar Malwares (software) para se infiltrar nos computadores de forma a assumir o controle da máquina, monitorar suas ações e até induzir o individuo a pressionar certas teclas, podendo enviar dados confidenciais de seu computador ou rede para a base do invasor. Uma forma a se evitar esses ataques com o fim de proteger seria investindo em práticas de segurança e entendendo as vantagens da segurança cibernética.

Assim diante do surgimento várias plataformas virtuais como WhatsApp, Messenger, Telegram, YouTube, Instagram e tantos outros, tornou-se mais ágil a comunicação com grande número de visualizações ao mesmo tempo, pois são interligados entre si, todos pertencem ao mundo da WEB, onde além da simples troca de texto, se tem a transmissão de arquivos em vários formatos, como documentos, imagens e vídeos, se tornando ainda mais atrativos a seus usuários,

Com o passar dos anos a tecnologia se tornou uma grande aliada dos pontos essenciais, através dela pôde-se proporcionar riquezas, agilizar os processos que muitas vezes eram morosos e mais dispendiosos, tudo se tornou mais rápido e preciso, e com isso um pouco menos dispendioso, possibilitando a renovação de forma crescente e continua, porém toda essa diversidade existente no meio cibernético podemos encontrar alguns meios ao qual gera problemas pessoais, empresariais, sociais, são os chamados Crimes Cibernéticos.

A opinião de Pinheiro em 2001 é a seguinte: (FIORILLO; CONTE, 2016, p.183, *apud* ASSUNÇÃO, 2018, pág. 03).

> Com a popularização da Internet em todo o mundo, milhares de pessoas começaram a se utilizar deste meio contemporaneamente se percebe que nem todos a utilizam de maneira sensata e, acreditando que a internet um

[2] Hacker é uma palavra da língua inglesa que, no âmbito da informática, designa alguém capaz de invadir dispositivos eletrônicos, redes e sistemas de computação, seja para verificar sua segurança, para aperfeiçoá-lo ou para praticar atos ilícitos.

[3] Os crackers são indivíduos que possuem um conhecimento elevado na área de tecnologia da informação, mas que utilizam suas habilidades em benefício próprio ou para prejudicar outras empresas e pessoas.

> espaço livre, acabam por e ceder em suas condutas e criando novas modalidades de delito: os crimes virtuais.

Ainda que muitas vezes a internet seja considerada como um território livre, onde não se tem lei e nem punição, porém, a realidade não se corrobora com esse entendimento, o judiciário vem coibindo a sensação de impunidade que reina no ambiente virtual e dessa forma no combate a criminalidade cibernética, com a aplicação do código penal, código civil e das legislações especificas.

Quando se faz uma análise sobre crimes cibernéticos, pode-se verificar uma ligação com a dignidade da pessoa humana, devido a limitação que sua forma pode causar, a limitação na forma de se expressar o pensamento, limita a liberdade de expressão através de formas variadas, gerando um conflito de interesses onde muitas vezes a pessoa pode ter seus direitos, suas garantias e suas intimidades invadidos.

> O conceito de "delito informático" poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade a confidencialidade (ROSSINI, 2004, p. 110 *apud* SENA, 2014, online).

O crime virtual deve ser analisado sob diferentes perspetivas por conta de suas peculiaridades se comparado com o "crime real" que tem local precisado e a ação pelas autoridades coatoras mais fácil, pois eles conseguem visualizar as provas de forma mais clara, já o crime virtual dispensa o contato físico entre vítima e agressor, ocorrendo em um ambiente sem povo, governo ou território, além de não gerar a princípio a sensação de violência para um segmento social específico pois não há padrões para o seu acontecimento. (SYNDOW,2009, *apud* CASTRO, 2022, online).

Nos crimes cibernéticos muitas vezes o real e o virtual não são opostos, passam a ser complementares, eles se fundem são muito próximos, ou seja, um crime cometido no real pode afetar o virtual e um crime no virtual pode afetar o real.

No Brasil se verifica ano após ano um grande aumento dos crimes cibernéticos e isso vem se tornando um desafio, pois muitas vezes ele ocorre pela falta de informação, de conhecimento e de segurança nos meios digitais, o grande aumento do uso de dados tecnológicos e digitais, e mesmo com a divulgação de novos crimes na rede, muitas vezes nem todos os indivíduos entendem como pode ocorrer,

pois abrange pessoas de todas as idade e níveis sociais, deixando desta forma os indivíduos mais vulneráveis, e como consequência muitas vezes são vitimas em situações como fraudes, vazamento de dados entre outros sem nem ao menos saber que ocorreu.

O princípio da legalidade consiste em um dos mais importantes do ordenamento penal brasileiro. Ele encontra-se positivado no art. 5º, inciso XXXIX da Constituição Federal de 1988: “Não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal”, e Art. 1º do Código Penal.

Devido a ausência de uma legislação especifica que aborda temática de crimes cibernéticos, cabe ao Direito Penal vigente julgar aquele que comete crime cibernético. Os crimes praticados via Internet serão julgados de acordo com sua forma, e cometimento é o que diz Wendt e Jorge o seguinte: “Os crimes cibernéticos consistem no cometimento de atividades ilícitas por meio do computador ou rede de internet e classificam-se de acordo com a sua forma de cometimento” (WENDT, JORGE, 2012, *apud* ASSUNÇÃO, 2021, pág. 08.)

Crime cibernético pode ser descrito como toda conduta, definida em lei como crime, em que o computador tenha sido utilizado como o instrumento para praticar o ato ou consistir em seu objeto material.

Nos crimes virtuais os indivíduos ultrapassam o bom senso, onde muitas vezes violam a dignidade da pessoa humana, mitigando seu exercício pleno, passando a possibilidade de infrações reais com exposição da intimidade, decoro social e a imagem do outro, gerando uma agressão do ambiente físico para o online, impossibilitando muitas vezes separar o que é real do virtual.

Normalmente o infrator se esconde por traz de uma tela para então cometer o crime, podendo se utilizar de vários meios de atuação, dentre eles ferir a dignidade ou até mesmo a honra da pessoa, onde muitas vezes o crime se dá como vingança, servindo como meio de punição por algo que ocorreu e não foi do agrado de uma das partes, exemplo disto é quando se tem o termino de um relacionamento muitas vezes por vingança uma das partes se publica fotos ou vídeos íntimos do outro gerando assim um grande constrangimento.

Dessa forma o que era para ser considerado como uma inclusão através da interatividade, passa a ser um problema ético de desrespeito ao direito da dignidade, havendo assim a necessidade de gerar regras protetivas, pois quanto

maior é a liberdade maior é a responsabilidade onde a privacidade abraça o posicionamento de relevo a proteção, criando uma barreira ao externo.

Os programas populares com maior utilização pelos invasores são: o vírus, o cavalo de troia, o Spyware, o Ransomware, o adware, Botnets, Malware, Phishing, e Ataque DDoS, entre outros, onde cada qual possui uma função especifica.

O Malware, nada mais é do que software (programa) malicioso, criado normalmente por um criminoso ou um hacker que tem por objetivo invadir os sistemas, podendo ser enviado por mensagens, email ou qualquer tipo de download, tendo no intuito de copiar dados privados ou até mesmo para extorquir uma vítima.

O Phishing (é conhecido como forma de pescar), ocorre quando e-mails de spam ou outras formas de comunicação são enviadas em massa, com a intenção de induzir os destinatários a fazer algo que prejudique a segurança deles ou a segurança da organização em que trabalham. Atuam com links e arquivos suspeitos, parecido com o malware, a principal proteção e atenção estão em rejeitar supostas propostas "fáceis", ou seja, propagandas de promoções vantajosas. Já o "***spear-phishing*"**, é um método mais profissional, onde o as mensagens são criadas para se parecer com mensagens de uma fonte confiável. Por exemplo, para parecer que vieram diretamente do CEO ou do gerente de TI da empresa. Tem menos aspecto visual para identificação da falsidade. (KOVACS, 2021, online)

Os Ataque DDoS, São um tipo de ataque cibernético que os hackers usam para paralisar um sistema ou uma rede. Os criminosos que fazem extorsões cibernéticas podem usar a ameaça de um ataque DDoS para exigir dinheiro. Outra utilização, o DDoS pode ser uma tática de distração enquanto acontece um segundo tipo de crime. Uma das formas de evitar a invasão destes programas seria a utilização de bons programas antivírus que devem ser atualizados frequentemente, seguindo o mesmo parâmetro que novos *malware* vão aparecendo, utilizar senhas fortes, com alto poder de proteção, manter o software, sistema sempre atualizado, em se tratando de dados bancários observar os extratos bancários. Porém muitas vezes nem mesmo tomando todos os cuidados de proteção podem ser eficientes para se evitar as invasões. (KOVACS, 2021, online)

Os crimes cibernéticos mais comuns são os de fraude, roubo de dados e informações diversas dos indivíduos, pornografia infantil, cyberbullying, pornografia de vingança, discurso de ódio, intolerância, entre outros.

De forma sociocultural pode-se dizer que em 2017, aproximadamente 62 milhões de brasileiros foram afetados por algum crime cibernético. Os usuários de smartphones e aplicativos WhatsApp são os maiores alvos dos cyber criminosos. **Phishing** é a prática mais comum usada por golpistas e inclui o envio de conversas ou mensagens falsas com links fraudulentos. Por exemplo, quando esse link é aberto, os dados do usuário podem ser roubados ou apontar para uma loja online. (DECCO-SEDIF, 2021, online).

Em janeiro de 2021 se teve um vazamento de dados de 223 milhões de indivíduos no Brasil, abrangendo praticamente todos os indivíduos, inclusive dados de pessoas falecidas, onde o vazamento dos dados pessoais pode ser de forma completa como o CPF, endereço, poder aquisitivo para compra, bens, inclusive fotos particulares, é relevante observar que através desses vazamentos de dados se pode ter a execução de outros crimes, como a solicitação de auxílio emergencial, solicitar empréstimos, fazer dividas, entre outros, é uma situação muito delicada, pois com a exposição total da pessoa fica difícil detectar o problema antes que os crimes aconteçam. (G1, 2012, online).

No caso Carolina Dieckmann que ocorreu em 2011, onde se teve fotos pessoais furtadas de seu computador pessoal por Crackers, através da implantação de uma isca (spam), onde permitiu sem querer que ele invadisse seu email e com isso ele furtou 60 arquivos, entre eles fotos intimas, tinha compartilhado com seu parceiro sendo divulgadas na internet, um dos suspeitos era menor de idade estava chantageando a atriz em 10 mil para que as fotos não fossem publicadas, diante de sua constante aclamação por justiça, gerou grande comoção popular e discursão sobre o assunto, diante disto foi proclamada a Lei Carolina Dieckmann (Lei 12.737/2012), lei que pune os indivíduos que difundir, transmitir fotos, vídeos íntimos ou algo que possa gerar qualquer tipo de constrangimento ao individuo.

> A Lei nº. 12.737/2012 se pune como crimes infrações ligadas ao meio informático, como por exemplo, invadir computadores, violar dados de usuários ou apenas destituir sites. O projeto de lei (PLC 35/2012) que deu origem a norma, já tinha sido pedido por empresas de financiamento e sistemas financeiros em decorrência da crescente quantidade de golpes executados pela internet. Com o fato da divulgação das fotos íntimas da referida atriz terem tido grande apelo popular, o projeto logo foi sancionado. (Lei 12.737 de 2012).

Os cibercrimes podem ser classificados como puros, mistos e comuns, onde:

Os puros são aqueles em que o computador é o principal alvo dos infratores. Ou seja, quando eles atacam um sistema pela invasão todo o sistema pessoal ou corporativo sofre o ataque.

Os mistos acontecem quando os invasores possuem como alvo tanto o computador como toda a rede, ou seja, os dois são utilizados como alvo para o cometimento do crime, eles são a arma para a prática de suas ações.

Os comuns eles não querem utilizar nem o computador nem a rede para o cometimento do crime, eles querem utilizar, o computador (a máquina) apenas como meio de se armazenar, guardar informações ilegais e furtadas de outras vítimas, servindo apenas como uma memoria de arquivo.

Alguns dos principais crimes cometidos na forma virtual são:

Crime contra honra, podendo ser calunia, injuria ou difamação;

Crime contra a liberdade pessoal e ameaça;

E o Crime de stalking, mais conhecido como crime de perseguição.

Quando verificamos as formas de cometimento dos cibercrimes, podemos verificar uma lista gigantesca, dentre eles podemos verificar alguns como:

O de furto qualificado mediante fraude ou Confiança, que é a clonagem de cartão, como ocorreram muitas compras na internet principalmente durante a pandemia, e começaram a utilizar seus cartões para fazer compras online, assinar strimim de vídeo, serie de filme, daí seus dados ficam armazenados em site e posteriormente, esses crackers criminosos raqueiam seus dados, fazem compras, assinaturas e os utilizam até mesmo para prática em fins ilícitos.

O Estelionato, onde os criminosos raqueiam seu nome e dados, onde muitas vezes a vítima é surpreendida quando olha sua conta bancária por exemplo, ficando apenas com o prejuízo. São os chamados 171 de internet.

O crime de exposição pornográfica não consentida, conhecida nos estados unidos como **revenge porn**, foi instituído no código penal em 2018, no art. 218-C, é quando se briga com um namorado ou namorada e por vingança divulga suas fotos sem seu consentimento.

Crimes de perfil fake (falso), para se usar de forma ilícita, (se passando por outra pessoa) é quando se inscreve em um perfil utilizando dados falsos com o intuito de se cometer crimes.

Vale relatar que por fazer um perfil falso não configura crime em si, mas ter como intuito de se esconder sua verdadeira identidade para o cometimento de algum

ato ilícito é crime, e isto gera uma das maiores dificuldades para se identificar o criminoso, pois normalmente eles não se utilizam de sua identificação real.

Falsidade ideológica, o usuário vai emitir ou alterar documento para se obter qualquer vantagem, por exemplo efetuar a alteração de códigos de barras de um boleto, o pix (QR cold falso), onde se acredita estar efetuando o pagamento para determinada pessoa, porém na realidade está sendo para um criminoso.

1.1 SEÇÃO SECUNDÁRIA

Legislação especifica aplicável aos crimes digitais

Muitas vezes acredita-se que crimes virtuais não possuem tipificação penal, ou seja, ao ser praticado não constitui crime, isso se dá pelo fato de não terem previsões legais no preambulo o verbo “internet”, levando as pessoas a suporem que esses crimes são impunes, porém quando é identificado o infrator de qualquer ato ilícito de forma virtual se tem uma sanção penal aplicada, levando em consideração sua tipificação e consumação.

Para que se consiga identificar o criminoso e poder obter uma maior agilidade em se poder puni-los, é necessário ter a contribuição das vítimas, eles devem se manifestar sobre o ocorrido, através de denuncias e boletins de ocorrências, pois muitas vezes as pessoas nem se dá conta de que foram vitimas de algum tipo de crime cibernético e para que se ocorra a identificação do infrator, inicialmente se deve pelo menos saber da existência do ocorrido, pois sem a devida informação fica difícil sua identificação, visto que os criminosos normalmente se utilizam de **Deep web** ou **Darck web**.

Deep web: São os chamados sites secretos, que não aparecem nas páginas de buscas, eles ficam invisíveis para a Surface (nome da linha), é a parte da internet onde a maioria dos dados de cadastros está armazenada. Ou seja, tudo que precisa de um login e senha ficam aqui, por exemplo os dados dos emails ficam armazenados aqui, tudo que precisa de senha.

Darck web: é a parte da internet que não pode ser detectada facilmente, é a parte mais profunda/obscura da internet, garantindo assim a privacidade e o

anonimato de seus usuários onde ocorre os piores crimes da internet como criminalidade infantil e tráfego de pessoas.

O delito virtual pode ser dividido em quatro tipos, crimes de informática próprios, crimes de informática impróprios, crimes de informática mistos e crimes de informática mediato ou indireto, trazendo uma classificação mais precisa de delito informático. (JESUS, MILAGRE, 2016, *apud* ASSUNÇÃO, 2021, pág.10),

> **a) crimes informáticos próprios:** em que o bem jurídico ofendido é a tecnologia da informação em si, para estes delitos, a legislação penal era lacunosa, sendo que, diante do princípio da reserva penal, muitas práticas não poderiam ser enquadradas criminalmente;
> **b) crimes informáticos impróprios:** em que a tecnologia da informação é o meio utilizado para agressão a bens jurídicos já protegidos pelo Código Penal brasileiro. Para estes delitos, a legislação criminal é suficiente, pois grande parte das condutas realizadas encontra correspondência em algum tipo penal;
> **c) crimes informáticos mistos:** são crimes complexos em que, além de proteção do bem jurídico informático (inviolabilidade dos dados), a legislação protege outro bem jurídico. Ocorre à existência de dois tipos penais distintos, cada qual protege um bem jurídico;
> **d) crime informático mediato ou indireto:** trata-se delito informático praticado para a ocorrência de um delito não informático consumando ao final. Em Direito Informático, comumente um delito informático é cometido como meio para a prática de um delito-fim ordem patrimonial. Como, por exemplo, no caso do agente que captura dados bancários e usa para desfalcar a conta corrente da vítima. Pelo princípio da consunção, o agente só será punido pelo delito-fim (furto) (JESUS; MILAGRE, 2016, *apud* ASSUNÇAO 2021, pág. 10).

Segundo o artigo 1º do Código Penal Brasileiro traz “Não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal” O referido artigo é bem claro, o qual crime é a violação de normas estabelecidas em lei e que ocorrendo a falta de norma, não se pode falar de crimes.

As leis para crimes cibernéticos surgiram com maior força a partir de 2012, quando houve uma pressão da mídia sobre o legislativo, referente ao ocorrido no caso da atriz Carolinne Dieckmann, razão pelo qual foi promulgada a Lei 12.737/2012 conhecida como Lei Carolinne Dieckmann que ainda gera discussões sobre sua promulgação, sendo subsequente a divulgação de fotos íntimas da atriz Carolina Dieckmann furtadas de seu computador por crackes/hackers, com isso a atriz por diversas vezes clamou por “justiça”. Na época os infratores foram localizados e indiciado por extorsão qualificada, furto e difamação.

A repercussão foi tamanha que após 6 (seis) meses da divulgação das fotos, foram promulgadas com mesma data às Leis Nº 12.735/12 e 12.737/12 em que se deu alterações e inclusões de artigos no Código Penal, Código Penal Militar e a

publicação da Lei 7.716/89 (Lei de Preconceitos), dessa forma iniciou-se a tipificação de algumas condutas mediante uso de sistemas eletrónicos e digital, contra sistemas informatizados;

> LEI Nº 12.735 - Art. 1º Esta Lei altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrónico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.(...)Art. 4º Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado. Art. 5 o inciso II do § 3o do art. 20 da Lei no 7.716, de 5 de janeiro de 1989, passa a vigorar com a seguinte redação:(...) II - a cessação das respectivas transmissões radiofónicas, televisivas, eletrónicas ou da publicação por qualquer meio. (Lei nº 12.735 de 30/11/2012).

A Lei dispõe sobre a tipificação de alguns dos delitos praticados de forma virtual e alterou e inclui alguns artigos no Código Penal Brasileiro é a Lei nº 12.737, de 30 de novembro de 2012, conhecida informalmente como “Lei Carolina Dieckmann”, pois anteriormente a esta lei eram apenas mecanismos preparatórios, ou seja, só o fato de se ter acesso ao dispositivo não era considerado crime e com a lei isso passou a ser tipificado como crime.

Essa Lei representa avanços significativos, onde se tem a aplicação de algumas penas pelo cometimento de crimes no âmbito virtual, porém, sua eficácia ainda é insuficiente.

A referida Lei incluiu o artigo 154-A, no Código Penal brasileiro, in verbis:

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

Uma das fragilidades é a qualificação do crime que está relacionado com a violação dos mecanismos de segurança, ou seja, se não possuir um mecanismo de segurança ou um meio de proteção, se deixa uma brecha para que não seja considerado crime.

O tipo penal utilizado seria invadir, porém ele nos direciona para a conduta física, de forma real, não podendo alcançar a conduta virtual, ondo o termo verbal correto seria utilizar acessar ou ter acesso.

A conduta descrita está direcionando ao fato de se ter como condicionante do modo a invasão a mediante violação de senha, bloqueio de tela, por exemplo, onde esse tipo penal emana com dolo, ou seja, ao invadir o agente deve ter a vontade de o

fazer, tendo com ele a vontade de obter algo, destruir, modificar dados, ou até mesmo deixar o sistema vulnerável para obtenção de vantagens indevidas. Dessa forma não se visualiza a conduta culposa como forma para punição de tal crime.

Castro, diz que:

> O tipo penal fora mal redigido e com o abuso de elementos normativos, contrariando a taxatividade. Dentre esses tipos penais elencados, o que se pode perceber é que todos possuem como elemento subjetivo a modalidade dolosa. Não quis o legislador brasileiro incriminar a modalidade culposa. O legislador da referida codificação, possui pouca informação sobre o sistema informático, e isso é agravado pala falta de reflexão por parte da Dogmática Penal Brasileira, refletindo a lacuna normativa e a falta de debate em torno da moralidade das condutas cibernéticas, bem como as consequências e prejuízos causados por essas condutas (CASTRO, 2018, *apud* ASSUNCÃO, 2021, pág. 12).

Porém mesmo com alguns pontos negativos, ela é considerada como um avanço de forma significativa para que se tenha novas reflexões e evolução em relação a referida Lei, é certo que ela necessita de algumas atualizações, visto que o ambiente virtual está em constante evolução e sendo assim os crackers estão sempre em busca de possíveis vítimas e na utilização cada dia mais com uma maior tecnologia a seu dispor.

Ao verificar a Lei na integra se pôde verificar que o legislador ao promulgá-la não se preocupou com os cybercrimes em espécie, mas sim com o momento, o qual uma pessoa com fama pública teve suas imagens íntimas divulgadas e visando uma proteção própria.

Os demais crimes virtuais continuaram a ser julgados tendo como base os efeitos danosos causados pelos infratores, ou seja, a falta de uma lei que classifica e pune não é o real problema dos crimes cibernéticos, mas sim nas questões técnicas de como se chegar ao infrator, e também em se saber de quem é a competência para julgar tal crime.

Em 2014 teve a promulgação da Lei de nº 12.965/2014, foi um Marco Civil na Internet, pois trouxe para o ordenamento jurídico o princípio da neutralidade de rede e reforçou a comunicação, a manifestação de pensamento e o princípio da liberdade de expressão, já consagrada de forma constitucional, agora de forma mais abrangente gerando uma nova cultura de respeito a esse princípio, visando uma maior liberdade e menor controle estatal, sendo de essencial importância para os avanços tecnológicos do país, onde delimitou deveres, direitos, garantias e princípios para o

uso da internet, ofereceu diretrizes para a atuação da União, Estados, distrito Federal e Municípios.

Ela é um amparo legal relacionado aos crimes cibernéticos, pois além de proteger os dados de privacidade dos usuários ele oferece para as vítimas poder exigir retirada do conteúdo indesejáveis da rede.

No ano de 2018 se teve a promulgação da Lei 13.709/2018 Lei LGPD (Lei Geral de Proteção de Dados), onde seu principal objetivo é proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo. Onde a lei diz que o princípio da segurança é quando:

> [...] se tem a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão. [...] Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais. (Lei 13.709/2018 – Lei LGPD).

Em 28 de maio de 2021, foi sancionada a Lei 14.155, onde modifica e inclui alguns dispositivos do Código de Processo Penal referentes aos crimes de invasão de dispositivos informáticos, agravando penas como invasão de dispositivo, furto qualificado e estelionato mediante fraude eletrónica, dentre outros. Ela atualizou a Lei Carolina Dieckmann, modificando o tipo penal do delito e incluiu formas qualificadas e majoradas ao furto mediante fraude e ao estelionato, tornando assim as punições um pouco mais rígidas.

Segundo Sidney, presidente da Febraban em entrevista para Law Innovation em 31/05/2021, após a publicação da Lei 14.155, diz que:

> os golpes cometidos em meios digitais terão penas que podem chegar a até oito anos de prisão, agravadas se os crimes forem praticados com o uso de servidor mantido fora do Brasil, ou ainda se a vítima for uma pessoa idosa ou vulnerável. [...] Para a Febraban (Federação Brasileira de Bancos), a tipificação do crime digital é um passo muito importante e necessário para coibir delitos cometidos no mundo digital e punir com rigor as práticas desses crimes, que levam muita dor de cabeça e causam grande prejuízo financeiro para o consumidor. [...] o furto mediante fraude por meio de dispositivo eletrônico, com ou sem a violação de mecanismo de segurança, ou o uso de programa malicioso, ou por qualquer outro meio fraudulento, tem pena de reclusão de 4 a 8 anos, acrescido de multa. A pena aumenta-se de um terço a dois terços se o crime for praticado com o uso de servidor mantido fora do Brasil, e de um terço ao dobro, se o crime for praticado contra idoso ou vulnerável. (SIDNEY, 2021, online)

Esta Lei gerou algumas alterações referente alguns tipos de penas e regimes, penas que antes eram somente detenção passando para reclusão, o regime inicial era semiaberto ou aberto, passou a ser regime fechado, anteriormente a falta de controle de qualquer tipo poderia ser usada para tentar desqualificar o crime, como

exemplo a simples falta de senha no celular da vítima, com a nova Lei isso cai por terra, passando a ser crime toda violação de dispositivo eletrônico com ou sem violação do mecanismo de segurança.

Quando nos referimos a crianças e adolescentes, tanto no Brasil como em várias partes do mundo, pode-se verificar publicações referente a criança e adolescente que tiram a própria vida por não conseguir conviver com a vergonha e o medo diante de ameaças de publicações colhidas via internet e frequentes ataques de cyberbullying, que ocorrem até mesmo entre as pessoas de sua convivência escolar ou de fora dela, gerando tamanha pressão em que eles se veem ameaçados por algo que não possuem maturidade suficiente para poder lidar.

A exposição de crianças e adolescente na internet ocupa a 5ª posição no ranking do disque 100, incluindo casos de pedofilia, cyberbulliing e pornografia infantil, relata ainda que mesmo apesar dos registos o número pode ser ainda maior. (Ministérios dos Direitos Humanos e da Cidadania, 2020, online).

E diante disto e com o intuito de se proteger as crianças e adolescentes, o Ministério da Mulher, da Família e dos Direitos Humanos, lançou campanha para conscientizar as famílias sobre os riscos da exposição de crianças na internet. A campanha inclui materiais publicitários divulgados na internet, rádio e TV. O material foi produzido para incentivar pais e responsáveis a orientarem os filhos sobre o uso das tecnologias na proteção contra criminosos que atuam na internet. (Ministérios dos Direitos Humanos e da Cidadania, 2020, online).

E com o intuito de proteger as crianças e adolescente, a Câmara dos Deputados criou um projeto de Lei 4054/21 onde se tem regras para se evitar o linchamento virtual de crianças e adolescentes, essa proposta foi inspirada em casos de adolescentes que cometeram suicídio após publicar vídeo e ser alvo de críticas em aplicativo, esse Projeto de Lei estabelece medidas para combater crimes de ódio e preconceito praticados contra crianças adolescentes na internet.(Fonte: Agência Câmara de Notícias, 2022, online).

Em 31 de março de 2021, foi sancionado a Lei 14.132, Lei de Crime de perseguição ou stalking, onde foi inserindo o art. 147-A no Código Penal, que tem como finalidade tutelar a liberdade individual que é abalada por condutas que tem como finalidade o constranger da vítima por qualquer meio de ameaça de sua integridade física ou psicológica, onde muitas vezes a vítima era privada da liberdade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de

liberdade ou privacidade. Onde o elemento nuclear é classificado pelo verbo perseguir, que tem como objetivo de atormentar, importunar, aborrecer sua vítima.

Os delitos atuais não se limitam apenas a crimes patrimoniais conforme acontecia com estelionato e fraudes, com o passar dos anos e a expansão das redes sociais, as condutas criminosas passaram a ofender o íntimo da vítima, gerando transtornos e danos graves alem de infortúnios indo além do ambiente virtual.

Como os crimes virtuais podem ocorrer através de vários meios, quando se tem o dano da imagem, a exemplo em hipóteses que se utiliza *memes* ligados a imagem de alguém a fim de configurar deboche ou curtição, dependendo de como é a veiculação do *meme* a imagem pode gerar ofensa e constrangimento a essa pessoa.

Seguindo essa mesma linha o legislador ao prever leis que tratem especificamente sobre acontecimentos no ambiente virtual é essencial tutelar as garantias fundamentais previstas em texto constitucional previsto no Art. 5º caput e inciso X, da Constituição Federal do Brasil/1988.

> **Art. 5º**. Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> **X** - São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação. (Constituição Federal, 1988).

Portanto, o Legislativo não busca regulamentar apenas o ambiente virtual, mas as ferramentas essenciais para a manutenção de um sentimento mínimo de segurança jurídica, principalmente quando se trata da dignidade do individuo e todas as garantias constitucionais.

Quando se tratar de reparação por danos morais pelo uso da imagem, é de grande valia citar a sumula 403 do Superior Tribunal de Justiça (STJ), de 2009, que aduz que a indenização pela publicidade de uma imagem não autorizada pela pessoa para fins económicos ou comerciais independe da prova do prejuízo. Ou seja:

> […] o direito à imagem reveste-se de duplo conteúdo: moral, porque direito de personalidade; patrimonial, porque assentado no princípio segundo o qual a ninguém é lícito locupletar-se à custa alheia. Não há como negar a reparação à autora, na medida em que a obrigação de indenizar, em se tratando de direito à imagem, decorre do próprio uso indevido desse direito, não havendo, ademais, que se cogitar de prova da existência de prejuízo[...]. (TEIXEIRA, 2002, pág. 05).

Assim, quando já caracterizado um crime por utilização da imagem de forma não autorizada visando obter ganhos financeiros, neste caso fica dispensado a necessidade de se observar quais foram suas consequências, se foi ofensivo ou não.

Atualmente ainda não se tem uma definição exata sobre os crimes cometidos no âmbito virtual, pois as nomenclaturas e as definições são diversas, principalmente por conta da grande gama de ilícitos cometidos por meio da internet.

A conduta pode ser típica e ilícita, constitutiva de crime ou contravenção, culposa ou dolosa, comissiva ou omissiva, praticada por pessoa jurídica ou pessoa física, com uso em ambiente de rede, de informática que tem por elementos a disponibilidade, a integridade e a confidencialidade.

> Estamos em um momento muito diferente, com uma nova criminalidade digital. Existe a apropriação de imagens, a apropriação de dados, sem falar no problema das criptomoedas, que têm sido muito utilizadas na lavagem de dinheiro", opinou o ministro. "É uma realidade para a qual o Judiciário ainda não está preparado. Ele vai ter de se adaptar, criar mecanismos de enfrentamento e se aparelhar não só de forma material, mas também de forma técnica". (REIS JÚNIOR, 30 de junho de 2022)

O Legislativo também deve ter a obrigação de acompanhar os crimes virtuais e nos próximos anos o Judiciário brasileiro terá de se atualizar para combater os delitos digitais, pois não estão conseguindo acompanhar a evolução digital quando se refere a forma material, e técnica.

Essa realidade referente aos crimes cibernéticos provocou o Estado brasileiro a legislar sobre o assunto, levando com que esse tipo de crime passasse a integrar a seara do direito penal quando se tinha a impressão de ser impossível esse alcance pelo direito em razão da dificuldade de localizar os responsáveis pelos danos causados.

Porém, segundo entendimento de Valin, o maior problema está no fato da rede ter caráter internacional, onde na internet não se tem fronteiras, desta forma, tudo que se publica em rede estará disponível para visualização em todo o mundo, e de forma muito rápida não possuindo meios de se bloquear e delimitar seu alcance. Pensando nisso como devemos determinar o juízo competente para estudar um caso referente a um crime ocorrido na rede? (VALIN, ARAS, 2001, *apud* CARDOSO, 2017, online).

É importante verificar que os cibercrimes cometidos no Brasil, não causam efeitos apenas em território brasileiro, pois devido a rapidez de sua propagação ao qual é cometido, poderão afetar outros países quase que de forma imediata.

Quando falamos de competência relativo a estes crimes, devemos primeiramente entender o ambiente em que se praticam as condutas criminosas, e como nossa legislação ainda é um pouco carente referente a crimes cibernéticos, pois possui apenas pequenos fragmentos do que seria um crime cibernético, ficando a mercê da legislação indicá-las pois ainda não temos nenhuma característica oficial a respeito, as falhas relacionadas a crimes virtuais/cibernéticos, está relacionado a questões as técnicas de como se chegar aos infratores e em saber de quem é a competência para julgar o crime, pois a lei trata apenas de conceitos básicos, não traz peculiaridades, como prova e competência, só traz o dispositivo verbal, não se tem um rol taxativo sobre o que realmente seria um crime cibernético

Através de se observar como funciona e verificar o lugar onde ocorreu o crime, por quanto tempo se proliferou e qual foi sua duração no espaço, dessa forma se teria uma forma mais clara de quem seria a competência para julgar essas ações.

O Senado possui um projeto de Lei em tramitação que visa **reformar Código penal Brasileiro** o **Projeto Lei nº 236/12**, onde teria um capítulo exclusivo sobre crimes cibernéticos, dando uma maior amplitude sobre tal crime.

Referente a competência para julgar os crimes cibernéticos atualmente eles se dividem entre a Justiça do Estado e Justiça Federal, onde:

Será da competência Estadual, quando se tratar de crimes que não haja conflitos de competência, ou seja, um autor deve estar dentro do próprio Estado, dentro do mesmo espaço geográfico, seu IP deve ser reconhecido dentro do mesmo Estado.

É importante ressaltar, que nos crimes plurilocais onde a conduta tenha sido efetuada em mais de um local, será considerado o local dos últimos atos executórios, para a definição da competência sob a égide de crime na forma tentada. O qual entende que felizmente, a jurisprudência vem abrandando, de forma excecional, o rigor da teoria do resultado, para permitir a competência do Juízo em que foi praticada a ação delituosa, ainda que tenha sido outro o lugar da consumação, frente à necessidade de se preservar o máximo o conjunto de provas disponível. (OLIVEIRA, 2011, pág. 266 - 267).

Dessa forma quando se tem a possibilidade de se identificar onde está a máquina utilizada pelo agente criminoso, fica mais fácil visualizar de quem será a competência, pois seria esse o local onde ocorreu o crime.

Já a competência Federal será quando houver transacionalidade (elimina a fronteira), ou seja, o crime deve acometer mais de um país.

Diante disto, é plausível a necessidade de o Brasil buscar cooperação internacional para que se possa investigar, julgar e punir tais crimes, pois devido ao modo a que se efetua e o meio utilizado para consumação a conduta pode alcançar vários países. No ano de 2021 o Brasil aderiu sua participação na Convenção de Budapeste, celebrada em novembro de 2001 na capital da Hungria, entre as questões tratadas estão a criminalização de condutas, normas para investigação, produção de provas eletrônicas e meios de cooperação internacional. Decreto nº 11.491/23 traz a decisão, foi publicado no Diário Oficial da União (DOU), no dia 12 de abril de 2023.

No caso em que o crime for efetuado em território nacional e o resultado ocorrer em outro país se aplica a teoria da ubiquidade prevista no art. 6º do Código Penal Brasileiro, o foro competente a julgar será tanto o lugar onde foi efetuada a ação ou omissão, quanto o lugar onde se produziu o resultado. Desta forma, o foro competente será o do lugar onde foi praticado o último ato de execução no Brasil (art. 70, § 1º), ou o lugar no estrangeiro onde se produziu o resultado. (CAPEZ, 2012, Pág. 277. *Apud* CARDOSO, 2017).

1.1.1 SEÇÃO TERCIÁRIA

Jurisprudência existente sobre os crimes virtuais nos tribunais brasileiros.

Conforme relatado anteriormente muitos dos crimes cometidos no ambiente virtual já estão tipificados no Código Penal com o intuito de combater a criminalidade, porém mesmo estando no enquadramento tipificado, carecem de ajustes para maior abrangência, pois esses tipos se encontram em constante crescimento.

Neste capítulo visa explanar a forma de atuação dos tribunais em relação aos crimes virtuais, mesmo quando a legislação especifica possui carência legislativa. Serão expostas algumas jurisprudências pertinentes em relação aos crimes virtuais.

Segue abaixo jurisprudência referente a um crime virtual de divulgação de imagens e danos morais:

> **AGRAVO INTERNO NO AGRAVO EM RECURSO ESPECIAL. INDENIZATÓRIA. DECISÃO MANTIDA. RECURSO DESPROVIDO. AFRONTA AOS ARTS. 128 E 460 DO CPC/73. AUSÊNCIA DE PREQUESTIONAMENTO. ADMISSÃO DE PREQUESTIONAMENTO FICTO. NECESSIDADE DE INDICAÇÃO DE AFRONTA AO ART. 1.022 DO NCPC. DIVULGAÇÃO DE IMAGENS COM FINS ECONÔMICOS. DANOS MORAIS E MATERIAIS. CABIMENTO. AGRAVO DESPROVIDO.** 1. Esta Corte de Justiça, ao interpretar o art. 1.025 do Código de Processo Civil de 2015, concluiu que "a admissão de PRE questionamento ficto (art. 1.025 do CPC/15), em recurso especial, exige que no mesmo recurso seja indicada violação ao art. 1.022 do CPC/15, para que se possibilite ao Órgão julgador verificar a existência do vício inquinado ao acórdão, que uma vez constatado, poderá dar ensejo à supressão de grau facultada pelo dispositivo de lei". 2. O eg. Tribunal de origem adotou posicionamento consentâneo com a jurisprudência do Superior Tribunal de Justiça no que tange à indenização a título de dano material, que entende que a divulgação de imagem com fins econômicos, sem autorização do interessado, acarreta dano moral in reipsa, bem como dano material, sendo devida a indenização e desnecessária a demonstração de seu prejuízo material ou moral. Precedentes. 3. Agravo interno a que se nega provimento **(AGRAVO EM RECURSO ESPECIAL Nº 1.346.273 – PR, Relator: Min. RAUL ARAÚJO, 2019)**

Este é um acórdão proferido pelo Superior Tribunal de Justiça (STJ) em um agravo interno no âmbito de um recurso especial, em que se discute a possibilidade de indenização por danos morais e materiais decorrentes da divulgação de imagens com fins econômicos sem autorização do interessado.

O Tribunal de origem decidiu que a divulgação de imagem com fins econômicos sem autorização do interessado acarreta dano moral *in reipsa* (ou seja, presumido), bem como dano material, sendo devida a indenização e desnecessária a demonstração de seu prejuízo material ou moral.

Conforme pode ser visto no julgado foi estipulado a indenização a título de dano material, visto que o entendimento de uma divulgação da imagem com fins económicos geral conjuntamente com danos morais, e conforma Sumula 403 do STJ, para se configurar danos morais neste caso não se tem a necessidade de se provar se houve ou não dano a pessoa, apenas o simples fato de se utilizar a imagem de alguém para fins económicos ou comerciais, sem sua autorização previa, já configura danos materiais ou morais.

Abaixo segue outra jurisprudência a respeito de crime contra a honra:

> **JUIZADOS ESPECIAIS CRIMINAIS. DIREITO PENAL. QUEIXA-CRIME. DIFAMAÇÃO. CRIMES CONTRA A HONRA. GRUPO DE WHATSAPP. INEXISTÊNCIA DE IMPUTAÇÕES DE FATOS DETERMINADOS CAPAZES DE CONSUBSTANCIAR, POR SI, A OCORRÊNCIA POTENCIAL DE LESÃO OU MÁCULA À HONRA OBJETIVA OU SUBJETIVA DOS APELADOS. CRIMES CONTRA HONRA NÃO CARACTERIZADOS. RECURSO CONHECIDO E PROVIDO**. 1) Cuida-se de recurso inominado interposto pelo apelante em face da r. sentença que julgou procedente a

> pretensão deduzida na queixa-crime para condená-lo como incursa a sanção do art. 139 do CP. 2) O apelante, a priori, suscita a incompetência do juízo em razão da necessidade de prova pericial. Segundo ele, as conversas que embasaram sua condenação foram extraídas de um grupo privado do whatsapp, do qual o recorrido embora participante, não ficou demonstrados nos autos que este foi quem postou as mensagens à ordem 7. No mérito, alega a atipicidade do crime de difamação, por ausência de comprovação de materialidade. 3). Os apelados apresentaram contrarrazões à ordem 90, requerendo a manutenção da sentença proferida pelo juízo a quo. 4). O Ministério Público ofereceu o Parecer à ordem 112, manifestando-se pelo acatamento da preliminar arguida pelo apelante para determinar a nulidade do processo desde o recebimento da queixa-crime no juizado de origem e o conhecimento da apelação para reformar a sentença do juízo a quo para absolver o apelante com fulcro no artigo 386, inciso III, do CPP por não constituir o fato infração penal. 4) A condenação se baseou unicamente em provas testemunhais, no entanto, deveria ter apreciado outros meios de prova. 5). PRELIMINAR DE NULIDADE: Inicialmente, registre-se que, não obstante o caráter sigiloso das mensagens mantidas por aplicativos que utilizam a internet, no caso dos autos, para ter prova da materialidade dos fatos, deveria haver perícia criminal, nos termos do art. 35 da Lei nº 9.099/95, das postagens apresentadas à ordem 7, ou estas serem submetidas a ata notarial, lavrada por tabelião, atestando a veracidade dos fatos em meio digital, nos termos do art. 384 do CPC. 6). Portanto, ausentes os elementos suficientes a confirmar a denúncia, a absolvição é medida que se impõe, nos termos do artigo 386, inciso II, do CPP. 7). Recurso conhecido e provido. 8). Sentença reformada. **(TJ-AP - APL: 00564548020168030001 AP, Relator: MARIO EUZEBIO MAZUREK, Data de Julgamento: 07/08/2018, Turma recursal).**

Este é um caso de recurso inominado interposto pelo apelante contra uma sentença que o condenou pelo crime de difamação, previsto no artigo 139 do Código Penal. O apelante argumenta que o juízo foi incompetente, uma vez que a prova apresentada contra ele foi extraída de um grupo privado do WhatsApp, e que não há provas suficientes para comprovar a materialidade do crime.

O Ministério Público manifestou-se pelo acatamento da preliminar arguida pelo apelante e pela absolvição do mesmo com base no artigo 386, inciso III, do Código de Processo Penal, por não constituir o fato infração penal.

A Turma Recursal acolheu a preliminar de nulidade e considerou que, para comprovar a materialidade dos fatos, deveria haver perícia criminal ou ata notarial atestando a veracidade dos fatos em meio digital. Como esses elementos não foram apresentados, a absolvição do apelante foi decretada com base no artigo 386, inciso II, do Código de Processo Penal, que prevê a absolvição em caso de ausência de prova suficiente da materialidade do crime.

Em resumo, a Turma Recursal entendeu que não havia elementos suficientes para comprovar a ocorrência do crime de difamação, uma vez que não foram apresentadas provas adequadas para comprovar a materialidade do fato. Fato importante em pontuar a necessidade de se conferir toda documentação necessária

para comprovação e como se crime onde se utilizou um dispositivo para o cometimento do crime a Ata Notarial ou até mesmo um laudo de perícia no aparelho é de estrema importância para a comprovação do fato, visto não basta apenas apresentar o aparelho de forma física perante o juiz. Dessa forma, a sentença foi reformada e o apelante foi absolvido.

Segue abaixo jurisprudência onde se teve a invasão de conta pessoal e contas comerciais relacionadas a uma conta de facebook:

> **RESPONSABILIDADE CIVIL. INVASÃO DE CONTA PESSOAL E CONTAS COMERCIAIS DO AUTOR NO FACEBOOK. HACKER QUE SE UTILIZOU DOS PERFIS PARA OFERTAR VAGAS FALSAS DE EMPREGO. INÉRCIA DO FACEBOOK EM TIRAR AS PÁGINAS DO AR APÓS NOTIFICAÇÃO DO AUTOR**. falha na prestação de serviços configurada. SISTEMA DE SEGURANÇA OFERECIDO QUE NÃO EVITA O ACESSO POR FRAUDADORES. INAPLICABILIDADE DA EXCLUDENTE DE RESPONSABILIDADE DE CULPA EXCLUSIVA DO CONSUMIDOR OU DE TERCEIRO. FORTUITO INTERNO INERENTE AO RISCO DA ATIVIDADE DESENVOLVIDA. requerido que não conseguiu desconstituir o direito do autor. dever de indenizar configurado. OCORRÊNCIA DE DANOS MORAIS. SITUAÇÃO QUE ULTRAPASSOU A ESFERA DO MERO ABORRECIMENTO. redução E MAJORAÇÃO do quantum indenizatório. impossibilidade. MANUTENÇÃO DO VALOR. MAJORAÇÃO DOS HONORÁRIOS ADVOCATÍCIOS. INVIABILIDADE. sentença MANTIDA. apelação 1 (requerido) conhecida E desprovida. apelação 2 (AUTOR) conhecida e desprovida. 1. Autor que comprova que suas contas foram invadidas por hacker, bem como que noticiou o fato ao réu que ficou inerte. 2. Falha na prestação do serviço. Dever de segurança não cumprido. Ferramentas fornecidas pelo requerido que não impossibilitam ataques de hackers. Inocorrência de excludente de responsabilidade de culpa exclusiva do consumidor ou de terceiro (art. 14, § 3º, II, CDC), pois a invasão por fraudador é risco inerente à atividade exercida pelo réu. 3. Danos morais comprovados. Manutenção do valor fixado na origem. (TJPR - 10ª C. Cível - 0026768-65.2021.8.16.0014 - Londrina - Rel.: DESEMBARGADORA ANGELA KHURY - J. 20.04.2022) **(TJ-PR - APL: 00267686520218160014 Londrina 0026768-65.2021.8.16.0014 (Acórdão), Relator: Angela Khury, Data de Julgamento: 20/04/2022, 10ª Câmara Cível, Data de Publicação: 26/04/2022).**

O caso em questão trata de uma ação de responsabilidade civil em que o autor teve suas contas pessoais e comerciais invadidas por um hacker que utilizou os perfis para oferecer vagas falsas de emprego, e o Facebook ficou inerte em retirar as páginas do ar após notificação do autor.

A sentença considerou que houve falha na prestação de serviços por parte do Facebook, uma vez que o sistema de segurança oferecido não evitou o acesso por fraudadores, e que não se aplica a excludente de responsabilidade de culpa exclusiva do consumidor ou de terceiro, já que a invasão por fraudador é risco inerente à atividade exercida pelo réu.

Além disso, a sentença reconheceu a ocorrência de danos morais, que ultrapassaram a esfera do mero aborrecimento. O valor da indenização foi mantido, não sendo possível sua redução ou majoração.

CONCLUSÃO

Diante do foi apresentado podemos entender que estamos em um momento diferente, onde a virtual chegou também ao direito penal, estamos diante de uma nova criminalidade, os chamados crimes digitais ou crimes cibernéticos, onde são os crimes efetuados com o uso de um computador, ou qualquer mecanismo eletrónico que possui ligação com o mundo digital, podendo ter a apropriação de imagens, de informações, de todos os dados pessoais, sem uma barreira que o detenha, pois qualquer um pode ser atingido desde o cidadão comum como o próprio Estado, gerando assim uma insegurança tanto para a sociedade como para o mundo Jurídico.

Houve tentativas fracassadas de projetos lei ou até mesmo publicações apressadas de legislações, como é o caso da Lei Nº 12.737/2012, sendo necessário cautela na instauração de um ordenamento sobre o tema, devido a constante evolução sofrida no mundo virtual. Devemos lembrar que o Código Penal Brasileiro é de 1940, neste período nem existia o sistema digital e dessa forma muito menos os crimes cibernéticos, se tem um Projeto de Lei nº 236/2012, que está em tramitação para que se tenha a uma reforma do Código Penal, onde se teria um capítulo completo sobre crimes cibernéticos, mas por enquanto nada foi definido.

Esse tipo de crime é uma nova realidade, que estamos vivenciando, e o judiciário não se encontra totalmente preparado, devendo se adaptar a esse novo mundo não só de forma material mas sim de forma técnica, a própria legislação também deve ser atualizada, pois a legislação que temos hoje não está preparada para este tipo de crime, como existe condutas atípicas que não podem ser punidas pelo princípio da legalidade ou da reserva legal, pois o que temos hoje no direito penal diz que crime é exatamente o que está previsto na lei, e no crime cibernético temos caminhos, procedimentos e ações que não estão tipificados em lei, mas que sabemos que o tipo final seria uma ilicitude, um proveito indevido.

Dessa forma devemos preparar o judiciário como um todo de forma humana e material, e o legislador terá que agir de forma mais rápido, pois esse tipo de criminalidade vai se atualizando a cada dia que passa, devendo ser mais ágil, o suficiente para acompanhar as mudanças ocorridas, criando novos mecanismos na lei não só para tipificar esses atos como também para propiciar a atuação efetiva do

judiciário, pois o que se tem hoje já seria ultrapassado para amanhã, então todo o poder judiciário, o poder da advocacia devem estar constantemente se atualizando, para poderem atender a todos.

A visão para este tipo de crime deve ser mais orgânica menos individual do processo, não podemos privilegiar nenhuma parte, pois é o judiciário que vai se aproveitar de uma justiça mais eficiente e efetiva.

REFERÊNCIAS

ALMEIDA, Francisco Lasley Lopes; VIEIRA, Steferson Gomes Nogueira; CAVALCANTI, Sabrina Correia Medeiros. **Criminalidade na era digital**. 2021. A ilicitude da prova obtida pelo acesso ao aparelho celular do preso em flagrante-Impasses jurisprudenciais. Disponível em:https://www.academia.edu/45613535/a_i_licitude_da_prova_obtida_pelo_acesso_ao_aparelho_celular_do_preso_em_flagrante_impasses_jurisprudenciais. Acesso em: 10 de set. 2022.

ALMEIDA, Jessica de Jesus; MENDONÇA, Allanna Barbosa; CARMO, Gilmar Passos; SANTOS, Kendisson Souza; MENESES, Luana Munique; AZEVEDO, Roberta Rayanne Doria. **Crimes Cibernéticos**. Cadernos de graduação. Disponível em: https://periodicos.set.edu.br/cadernohumanas/article/download/2013/1217. Acesso em: 20 de out. de 2022.

ANDRADE, Carlos Henrique Gomes; REZENDE, Paulo Izidio da Silva. **Os crimes cibernéticos e os seus efeitos na imagem do indivíduo**. Revista Científica Multidisciplinar Núcleo do Conhecimento. Ano 05, Ed. 11, Vol. 03, pp. 64-78. novembro de 2020. ISSN: 2448-0959. Disponível em: https://www.nucleodoconhecimento.com.br/lei/os-crimes-ciberneticos. Acesso em: 04 de set. de 2022

ARAGÃO, Jackson José Lima. Crimes Cibernéticos: **A prevalência do direito à dignidade da pessoa humana sobre o direito da livre expressão do pensamento**. Revista Processos Multidisciplinar, v. 2, n. 4, p. 541-566, 2021. Disponível em: http://periodicos.processus.com.br/index.php/multi/article/view/436. Acesso em: 06 de set. de 2022.

ARAUJO, Laíss Targino Casullo; REIS, Sérgio Cabral dos. **Responsabilidade civil dos provedores de conteúdo de internet.** Outubro de 2011. Disponível em: https://ambitojuridico.com.br/edicoes/revista-93/responsabilidade-civildosprovedores-de-conteudo-de-internet/#_ftn3. Acesso em: 05 de set. de 2022.

ASSUNÇAO, Ayume da Silva. **A tipicidade dos crimes cibernéticos no direito penal brasileiro: um estudo sobre o impacto da lei nº 12.737/2012 e a desconstrução de uma dogmática penal dos crimes cibernéticos**. Disponível em:https://repositorio.animaeducacao.com.br/bitstream/ANIMA/18570/2/TCC%202%20-%20Crimes%20Cibern%C3%A9ticos%20%281%29.pdf. Acesso em: 20 de set. de 2022.

BARROS, Antônio. **Conheça a evolução dos crimes cibernéticos**. Edição - Rosalva Nunes. Fonte: Agência Câmara de Notícias, 23/08/2006. Disponível em: https://www.camara.leg.br/noticias/89137-conheca-a-evolucao-dos-crimes-ciberneticos. Acesso em: 05 de jan. de 2023.

BRASIL. **Código de Processo Civil.** Brasília: Planalto, 2015. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em: 20 de out. de 2022.

BRASIL. **Código Penal.** Rio de Janeiro: Catete, 1940. Disponível em: https://www2.camara.leg.br/legin/fed/declei/1940-1949/decreto-lei-2848-7-dezembro-1940-412868-publicacaooriginal-1-pe.html. Acesso em 20 de out. de 2022.

BRASIL. **Constituição da República Federativa do Brasil:** texto constitucional promulgado em 5 de outubro de 1988, com as alterações determinadas pelas Emendas Constitucionais de Revisão nos 1 a 6/94, pelas Emendas Constitucionais nos 1/92 a 91/2016 e pelo Decreto Legislativo no 186/2008. – Brasília: Senado Federal, Coordenação de Edições Técnicas, 2016. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/518231/CF88_Livro_EC91_2016.pdf. Acesso em: 25 de set. de 2022.

BRASIL. **Decreto Lei Nº 11.491 de 12 de abril de 2023**. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm. Acesso em: 15 de abr. de 2023.

BRASIL. **Lei Nº 9.609/1998 - Conhecida como Lei do Software.** Brasília: Planalto 1998. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9609.htm. Acesso em: 05 de fev. de 2022.

BRASIL. **Lei n. 12.735 – Lei Azeredo.** Brasília: Planalto, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 05 de fev. de 2023.

BRASIL. **Lei nº 12.737/12, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 – Código Penal; e dá outras providências: Brasília, 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 23 de set. de 2022.

BRASIL, **LEI Nº 14.132 - Lei Crime De Perseguição.** Brasília: Planalto 31 de março de 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14132.htm. Acesso em: 05 de fev. de 2023.

BRASIL. **Lei 13.709/18 - Lei Geral de Proteção de Dados Pessoais (LGPD).** Brasília: Planalto, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 05 de fev. 2022.

BRASIL. **Lei 14.155/21 - Dispõe sobre invasão de dispositivo informático de uso alheio.** Brasília: Planalto, 2021. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm. Acesso em: 05 de fev. de 2023.

BRASIL. **Lei 13.185 – Lei do Programa de Combate à Intimidação Sistemática**. Brasília: Planalto, 2015. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13185.htm. Acesso em: 10 de set. de 2022.

BRASIL. **Lei n. 12.965 – Marco Civil da Internet.** Brasília: Planalto, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 10 de set. de 2022.

BRASIL. Ministério dos Direitos Humanos e da Cidadania. **Exposição de crianças e adolescentes na internet ocupa 5ª posição no ranking do Disque 100**. 2020. Disponível em: https://www.gov.br/mdh/pt-br/assuntos/noticias/2020-2/novembro/exposicao-de-criancas-e-adolescentes-na-internet-ocupa-quinta-posicao-no-ranking-de-denuncias-do-disque-100. Acesso em: 11 de fev. de 2023.

BRASIL. **Projeto de Lei do Senado n° 236, de 2012**. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/106404. Acesso em: 05 de fev. de 2023.

BRASIL. **Projeto de Lei nº 4054, de 2021**. Disponível em: https://www.camara.leg.br/propostas-legislativas/2307531. Acesso em: 05 de fev. de 2023.

BEZERRA, Clayton da Silva; AGNOLETTO, Giovani Celso. **Combate ao Crime Cibernético** – 1ª.ed.- Rio de Janeiro; Mallet Editora, 2020.

BRIZOLA, Fernando Cezar Nunes, JUSBRASIL, **Primeiros Casos Interessantes De Crimes Da Internet**, Publicado por Advocacia Direito Digital e Crimes Cibernéticos. Disponível em: https://fernandocbrizola.jusbrasil.com.br/artigos/393077456/primeiros-casos-interessantes-de-crimes-na-internet. Acesso em: 03 de jan. de 2023.

CÂMARA DOS DEPUTADOS. **Legislação atual já pune cyberbullying e cyberstalking, diz advogada à CPI**: Fonte: Agência Câmara de Notícias. 2016. Disponível em: https://www.camara.leg.br/noticias/482215-legislacao/atual/jápunecyberbulying-e-cyberstalking-diz-advogada-a-cpi/. Acesso em: 02 de jan. de 2023.

CÂMARA DOS DEPUTADOS. **Pec 17/2019** - **Câmara aprova em 2º turno PEC que inclui a proteção de dados pessoais na Constituição,** Fonte: Agência Câmara de Notícias. 2021. Disponível em: https://www.camara.leg.br/noticias/801696-CAMARA-APROVA-EM-2%C2%BA-TURNO-PEC-QUE-INCLUI-A-PROTECAO-DE-DADOS-PESSOAIS-NA-CONSTITUICAO. Acesso em: 03 de fev. de 2022.

CAPEZ, Fernando. **Curso de Direito penal: Parte Geral**. 16ª Ed. 2ª tiragem. São Paulo: Saraiva, 2012. Vol. I.

CASTRO, Thainer Cordeiro de. Crimes virtuais: **crimes cibernéticos e as considerações sobre a criminalidade na internet**. Conteúdo Jurídico. Brasília-DF: 03 junho 2022. Disponível em: https://conteudojuridico.com.br/consulta/artigos/58585/crimes-virtuais-crimes-cibernticos-e-as-consideraes-sobre-a-criminalidade-na-internet. Acesso em: 23 de fev. de 2023.

CARDOZO, Alexandro Gianes. **Competência nos crimes cibernéticos**. JUSBRASIL, 2017, online. Disponível em: https://www.jusbrasil.com.br/artigos/competencia-nos-crimesciberneticos/514359859. Acesso em: 13 de out. de 2022.

CIRIACO, Douglas. **Qual a diferença entre Internet e World Wide Web**. Canaltech, 25 de agosto de 2016. Disponível em: https://arquivo.canaltech.com.br/entretenimento/qual-a-diferenca-entre-internet-e-world-wide-web/. Acesso em: 05 de fev. de 2023.

CONVENÇÃO. **Convenção De Budapeste é Promulgada no Brasil**. Ministério da Justiça e Segurança Pública – gov.br. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/convencao-de-budapeste-e-promulgada-no-brasil#:~:text=Bras%C3%ADlia%2C%2017%2F04%2F2023,Crime%20Cibern%C3%A9tico%2C%20firmada%20em%20Budapeste. Acesso em: 03 de mai. de 2023.

CRUZ, Diego; RODRIGUES, Juliana. **Revista Científica Eletrônica Do Curso De Direito.** ISSN: 2358-8551 13ª Edição. janeiro de 2018 – Periódicos Semestral. Disponível em: http://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/iegWxiOtVJB1t5C_2019-2-28-16-36-0.pdf. Acesso em 23 de nov. de 2022.

DULLIUS, Aladio Anastácio; HIPLLER, Aldair; FRANCO, Elisa Lunardi. **Dos crimes praticados em ambientes virtuais.** Agosto de 2012. Disponível em: https://www.conteudojuridico.com.br/consulta/Artigos/30441/dos-crimes-praticados-em-ambientes-virtuais. Acesso em: 10 de set. de 2022.

G1. 28/012021. **Megavazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber.** Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml. Acesso em: 05 de nov. de 2022.

KOVACS, Leandro. **O que é um crime cibernético? 3 casos populares.** Disponível em**:** https://tecnoblog.net/responde/o-que-e-um-crime-cibernetico-3-casos-populares/ Acesso em: 21 de mar. de 2023.

NASCIMENTO, Talles Leandro Ramos. **Crimes Cibernéticos Conteúdo Jurídico**. Brasília-DF: 17 dez 2018, 05:15. Disponível em: https://conteudojuridico.com.br/consulta/Artigos/52512/crimes-ciberneticos. Acesso em: 26 set. de 2022.

NAZARENO, Claudio; PINHEIRO, Guilherme Pereira; (organizadores). **Legislação sobre acesso à informação, proteção de dados pessoais e internet** [recurso eletrônico]. – 1. ed. – Brasília: Câmara dos Deputados, Edições Câmara, 2020. (Série legislação; nº. 22). Disponível em: file:///Users/lucianapupulin/Downloads/legisla%C3%A7%C3%A3o_acesso_informa%C3%A7%C3%A3o_2ed.pdf. Acesso em: 26 de nov. de 2022.

OLIVEIRA, Eugênio Pacelli de. **Curso de Processo Penal**. 15ª Ed. Ver e atual. Rio de Janeiro: Lume Juris, 2011.

PINHEIRO, Bruno Vitor de Arruda. **As novas disposições sobre os crimes cibernéticos**. Uma análise acerca das leis 14.132 e 14.155/2021. Disponível em: https://jus.com.br/artigos/98006/as-novas-disposicoes-sobre-os-crimes-ciberneticos. Acesso em: 10 de jan. de 2023.

DECCO-SEDIF. Portal Do Conhecimento. **Crimes cibernéticos: evolução da legislação brasileira**. 04/06/2019. Disponível em: https://www.tjrj.jus.br/web/portal-conhecimento/noticias/noticia/-/visualizar-conteudo/5736540/6447772. Acesso em: 21 de mar. de 2022.

REIS JÚNIOR, Sebastião. **Judiciário ainda não está preparado para crimes virtuais**, **opina ministro do STJ**. Disponível em: https://www.conjur.com.br/2022-jun-

30/judiciario-nao-preparado-crimes-virtuais-opina-ministro. Acesso em: 27 de mar. de 2023.

SENA, Tel. **Crimes Virtuais: Uma Análise Jurídica No Brasil**. Jusbrasil, 2014. Disponível em: https://jus.com.br/artigos/32331/crimes-virtuais-uma-analise-juridica-no-brasil. Acesso em: 02 de jan. de 2023.

SENADO FEDERAL. **Aprovada adesão do Brasil à Convenção sobre o Crime Cibernético**. 2021. Disponível em: https://www12.senado.leg.br/noticias/materias/2021/12/15/aprovada-adesao-do-brasil-a-convencao-sobre-o-crime-cibernetico. Acesso em: 10 de fev. de 2022.

SIDNEY, Issac. **Lei endurece penas para crimes eletrônicos como clonagem no WhatsApp e phishing.** Em 31/05/2021. Disponível em: https://lawinnovation.com.br/lei-endurece-penas-para-crimes-eletronicos-como-clonagem-no-whatsapp-e-phishing/. Acesso em 13 de jan. de 2023.

SOUZA, Murilo. Projeto cria regras para evitar "**linchamento virtual" de crianças e adolescentes**. reportagem – Souza, em 07/02/2022. Disponível em: https://www.camara.leg.br/noticias/848745-projeto-cria-regras-para-evitar-linchamento-virtual-de-criancas-e-adolescentes/. Acesso em: 03 de jan. de 2023.

STAROBINAS, Marcelo. **Brasil é líder mundial em crimes cibernéticos**. Folha de São Paulo. 20/11/2002. Disponível em: https://www1.folha.uol.com.br/fsp/mundo/ft2011200205.htm. Acesso em: 05 de jan. de 2023.

STJ. **Agravo Em Recurso Especial**. AREsp 1346273 PR 2018/0203681-5. Relator: Ministro Raul Araújo. DJe 24/04/2019. JusBrasil, 2019. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stj/859551575. Acesso em 03 de fev. de 2023.

TEIXEIRA, Salvio de Figueiredo. **Embargos De Divergência Em Recurso Especial Nº 230.268-SP** (2001/0104907-7). Disponível em: https://www.stj.jus.br/docs_internet/revista/eletronica/stj-revista-sumulas-2014_38_capSumula403.pdf. Acesso em: 10 de jan. de 2023.

TJ-AP. **Apelação**. APL: 00564548020168030001. Relator: Mario Euzébio Mazurek, DJ: 07/08/2018. JusBrasil, 2018. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-ap/641681338. Acesso em: 03 de fev. de 2023.

TJ-PR. **Apelação**. APL: 00267686520218160014. Relator: Ângela Khury, DJ: 20/04/2022. JusBrasil, 2022. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-pr/1477576190. Acesso em: 03 de fev. de 2023.

WIKIPÉDIA. **A enciclopédia livre, Malware**. 2022. Disponível em: https://pt.wikipedia.org/wiki/Malware. Acesso em 22 de fevereiro de 2023.