UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS
FACULDADE DE DIREITO

O DIREITO DIGITAL E A PUNIBILIDADE DOS CRIMES CIBERNÉTICOS NO ORDENAMENTO JURÍDICO BRASILEIRO

GABRIEL FELIPE RIBEIRO HENDERSON SALLES

RIO DE JANEIRO
2022.2

GABRIEL FELIPE RIBEIRO HENDERSON SALLES

O DIREITO DIGITAL E A PUNIBILIDADE DOS CRIMES CIBERNÉTICOS NO ORDENAMENTO JURÍDICO BRASILEIRO

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de Bacharel em Direito, sob a orientação do **Professor Dr. Cezar Augusto Rodrigues Costa**.

RIO DE JANEIRO
2022.2

CIP - Catalogação na Publicação

S168d

Salles, Gabriel Felipe Ribeiro Henderson
O Direito Digital e a Punibilidade dos Crimes Cibernéticos no Ordenamento Jurídico Brasileiro / Gabriel Felipe Ribeiro Henderson Salles. -- Rio de Janeiro, 2022.
71 f.

Orientador: Cezar Augusto Rodrigues Costa.
Trabalho de conclusão de curso (graduação) - Universidade Federal do Rio de Janeiro, Faculdade Nacional de Direito, Bacharel em Direito, 2022.

1. Punibilidade. 2. Crimes cibernéticos. 3. Internet. 4. Direito Penal. 5. Direito virtual. I. Costa, Cezar Augusto Rodrigues, orient. II. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a), sob a responsabilidade de Miguel Romeu Amorim Neto - CRB-7/6283.

GABRIEL FELIPE RIBEIRO HENDERSON SALLES

O DIREITO DIGITAL E A PUNIBILIDADE DOS CRIMES CIBERNÉTICOS NO ORDENAMENTO JURÍDICO BRASILEIRO

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de Bacharel em Direito, sob a orientação do **Professor Dr. Cezar Augusto Rodrigues Costa**.

Data da Aprovação: 04 / 01 / 2023 .

Banca Examinadora:

Cezar Augusto Rodrigues Costa
Orientador

Francisco Ramalho Ortigão Farias
Membro da Banca

Nilo Cesar Martins Pompílio da Hora
Membro da Banca

RIO DE JANEIRO

2022.2

AGRADECIMENTOS

Gostaria de agradecer imensamente aos meus familiares por todo apoio e paciência durante todos os anos em que me dediquei, quase que exclusivamente, às atividades profissionais e acadêmicas necessárias para o meu crescimento, o que tem me possibilitado alcançar os meus maiores objetivos de vida. Agradeço ao meu pai, Marcelo Henderson Salles, por todo o suporte e estrutura, que foram essenciais para que eu pudesse me aprimorar e vencer às adversidades que enfrentamos nos últimos anos. Sou absurdamente grato à minha mãe, Eliane Ribeiro da Rocha Salles, pela paciência, empatia, amor e companheirismo, mesmo diante de todos os obstáculos e surpresas que surgiram no nosso caminho. Agradeço aos meus avós, irmãos, primos, amigos e colegas que sempre confiaram no meu potencial e nunca desacreditaram da minha força e capacidade de alcançar grandes feitos. Os momentos experienciados na Faculdade de Direito foram muito construtivos, engrandecedores e positivos para minha formação, tanto como profissional quanto como pessoa, de forma que tenho muito a agradecer por essas oportunidades. Agradeço também ao meu professor, orientador e inspirador, Dr. Cezar Augusto Rodrigues Costa, pela oportunidade de trabalhar em parceria neste projeto e por me acompanhar em mais um grande passo para o meu futuro. Carregarei com orgulho a honra de ter sido parte da Faculdade Nacional de Direito - UFRJ.

Muito obrigado!

RESUMO

O presente trabalho reflete acerca da aplicação dos dispositivos penais aos crimes cibernéticos no âmbito do ordenamento jurídico brasileiro, bem como analisa o surgimento de novos institutos penalizadores mais específicos, com intuito de punir e coibir tais práticas. A análise será realizada a partir do surgimento da ideia de Direito Virtual e da definição de crimes cibernéticos, perpassando pelo conceito e pelos aspectos históricos desses delitos, os quais são decorrentes da acelerada globalização e das grandes inovações tecnológicas do século. São investigados diversos crimes que são comuns no ciberespaço, como a pornografia infantil e divulgação de material pornográfico, o estelionato e outros tipos de fraude, a invasão de privacidade (incluindo o phishing), os crimes contra a honra, entre outros. Além disso, busca analisar os movimentos legislativos para criação de normas mais específicas e eficazes no que tange à repressão dos crimes cibernéticos no Brasil, assim como observar as principais dificuldades enfrentadas pelos legisladores e aplicadores do direito nesse processo. O principal objetivo do estudo é identificar quais os mecanismos de punição aos crimes cibernéticos existentes, gerais ou específicos, bem como avaliar sua eficácia perante o crescimento da internet e intensificação das relações virtuais.

Palavras-chave: Punibilidade – Crimes cibernéticos – Internet – Direito Penal – Brasil – Direito virtual – Tecnologia

ABSTRACT

The work reflects the application of the criminal provisions presented cyber no scope of crimes, as ordering regarding new more specific Brazilian legal provisions, with punitive institutes and specific new restraints. The analysis will be based on the concept of definition and what are the ideas of Virtual Law and the series of cybercrimes, through the concept of concept and the historical aspects, which are created by the innovation of the great technological innovations of the century. Several crimes that are common in cyberspace are investigated, such as child pornography and dissemination of pornographic material, embezzlement and other types of fraud, invasion of privacy (including phishing), crimes against honor, among others. In addition, I analyze the legislative movements, as well as the main difficulties faced by legislators and applications of the process. The main objective is to identify which mechanisms to study existing cybercrimes, general or specific, as well as to evaluate the internet and intensify the attempt to study virtual relationships.

Keywords: Punishment – Cybercrimes – Internet – Criminal Law – Brazil – Virtual law – Technology.

SUMÁRIO

INTRODUÇÃO 8
1. O ADVENTO DA INTERNET E DOS CRIMES CIBERNÉTICOS 10
1.1 ASPECTOS HISTÓRICOS 10
1.2 ACEPÇÃO DE CRIMES CIBERNÉTICOS 122
1.3 PRINCÍPIOS DO DIREITO PENAL BRASILEIRO E O CYBERCRIME 166
2. DOS DIREITOS À PRIVACIDADE E INTIMIDADE NA INTERNET 19
2.1 MARCO CIVIL DA INTERNET: PRINCÍPIOS DA REDE NO BRASIL 25
2.2 PROTEÇÃO DE DADOS PESSOAIS NA INTERNET 28
3. ASPECTOS GERAIS DOS CRIMES DIGITAIS E AS LEGISLAÇÕES ESPECÍFICAS 36
3.1 DAS PROVAS E RASTROS 37
3.2 DO CONCEITO DE CRIME, DOS CRIMES VIRTUAIS E A SOCIEDADE 38
3.3 SUJEITOS DOS CRIMES CIBERNÉTICOS 400
3.3.1 Do sujeito ativo 400
3.3.2 Do sujeito passivo 422
3.4 DO LOCAL E O TEMPO 43
3.5 LEGISLATIVA BRASILEIRA 45
3.5.1 Novos tipos de crimes cibernéticos 47
3.5.2 Delegacias especializadas em crimes informáticos 52
4. UMA ANÁLISE JURISPRUDENCIAL DOS CRIMES VIRTUAIS 54
CONCLUSÃO 63
REFERÊNCIAS 65

INTRODUÇÃO

O tema a ser debatido neste estudo, a punibilidade dos crimes cibernéticos no ordenamento jurídico brasileiro, será apresentado levando-se em consideração o sistema normativo jurídico e a legislação específica nacional, especialmente no que tange à realidade social de grande dependência e engajamento da sociedade à rede mundial de computadores e às novas tecnologias, assim como o consequente aumento expressivo de crimes cometidos virtual e anonimamente.

Portanto, após uma breve ambientação histórica e definição teórica dos crimes cibernéticos, o presente trabalho buscará analisar qualitativamente os cibercrimes sob a ótica do Direito Penal Brasileiro, trazendo a reflexão sobre como se dá a proteção dos direitos individuais e dos bens jurídicos tutelados no ambiente virtual, de forma analítica.

Deste modo, ao longo dos primeiros capítulos, será exposto o avanço da ideia de punibilidade dos crimes cibernéticos no ordenamento jurídico brasileiro, com a análise dos princípios constitucionais relevantes ao debate da matéria, como os direitos à intimidade, privacidade, liberdade e honra.

Por conseguinte, será apontado como vem se desenvolvendo os dispositivos legislativos, que objetivam acompanhar a acelerada popularização da internet e os problemas decorrentes de seu mau uso. O objetivo da pesquisa será investigar a aplicabilidade e adaptabilidade da lei em sentido amplo, principalmente no que tange às especificidades e facilidades dos delitos cometidos no ciberespaço, assim como ponderar acerca das lacunas legislativas ainda existentes no que se refere ao tema.

Visando alcançar efetivamente o objetivo apontado, será realizada uma pesquisa doutrinária e legislativa, paralelamente com a análise das normas e princípios, nacionais e internacionais, que versem sobre o assunto, de forma a construir um contexto geral do assunto. Esse estudo servirá como base para expor a relação entre a legislação vigente, específica ou secundária, e a efetiva punibilidade dos crimes virtuais, analisando a simultaneidade entre a evolução da internet e o consequente aumento da prática dos ilícitos cibernéticos, bem como buscará ponderar a respeito do desenvolvimento e aplicação dos dispositivos penais.

Por fim, após uma reflexão crítica acerca da aplicabilidade, abrangência, tratamento e regulamentação dos crimes cibernéticos no ordenamento jurídico brasileiro, será realizada a análise jurisprudencial desses delitos, de forma a expor os entendimentos dos tribunais no julgamento dessas infrações, o que buscará concluir a investigação do tema, com as respectivas considerações finais.

1 O ADVENTO DA INTERNET E DOS CRIMES CIBERNÉTICOS

1.1 ASPECTOS HISTÓRICOS

A rede mundial de computadores, assim como os dispositivos tecnológicos que são capazes de acessá-la, como computadores e notebooks, celulares e até mesmo aparelhos televisores, surgem com o objetivo de trazer praticidade e facilidades à vida das pessoas. É possível estabelecer conexões e se comunicar quase que instantaneamente, assim como a tecnologia já nos permite até mesmo ver e ouvir outros indivíduos em tempo real e gratuitamente, seja por chamada de vídeo ou de áudio, o que está cada vez mais comum e acessível. Tais dispositivos são aparelhos que nos permitem receber e enviar informações, cada um com suas próprias características, especificidades e limitações, de acordo com cada forma de tecnologia.

A história da internet se inicia quando, em meados da década de 1960, os Estados Unidos buscavam formas de criar um sistema que pudesse conectar longas distâncias para a transferência de dados sem a interferência ou interceptação de terceiros durante a chamada "Guerra Fria", principalmente para a troca de informações de maneira sigilosa.

Com isso, surgiu o primeiro projeto informático chamado "Arpanet", que após diversas mudanças e inovações, nos levaria a internet como conhecemos hoje. A partir da década de 70, a internet começou a se popularizar de maneira descontrolada, de modo que se tornou muito mais acessível e barata, mas isso trouxe também as primeiras ocorrências do que denominamos como crimes virtuais.

Não é possível precisar com certeza quando surgiu o primeiro "vírus de computador", porém acredita-se que o "Programa Creeper" foi o pioneiro nesse tipo de software malicioso, tendo sido criado no ano de 1971. De acordo com Dácio Castelo Branco (2021), o projeto foi criado por Bob Thomas, e tinha por objetivo testar a segurança de sistemas, sem um motivo específico. Surgiram vários outros programas com intuito malicioso ou delitivo ao longo dos

anos, que objetivam desde a invasão de sistemas até o roubo ou divulgação de informações sensíveis. Por outro lado, também foram criados diversos outros mecanismos de proteção e de simplificação no uso da internet para os usuários comuns, que são aqueles que não são especialistas em informática. Podemos citar, por exemplo, os antivírus e os antimawares, que são softwares responsáveis por localizar, bloquear e excluir os programas e arquivos maliciosos do dispositivo, ou até mesmo identificar e bloquear invasores. Acredita Roseli Andrion (2021) que o primeiro antivírus do mundo foi criado por Fred Cohen em 1983, como parte de um experimento para sua tese de doutorado.

Com o intuito de facilitar e popularizar ainda mais o uso da internet, juntamente com os navegadores de internet, que são softwares que permitem navegar entre páginas e sítios por meio de links sucessivos, foram criados também os motores de busca, que são ferramentas que permitem filtrar e localizar informações no âmbito da Web, bem como mostra-las de maneira simplificada e organizada ao usuário. Neste sentido, esclarece Brookshear (2013, pag. 09) que:

> "Para tornar a informação na Web acessível, sistemas de software, chamados de motores de busca, foram desenvolvidos para ''peneirar'' a Web ''categorizar'' seus achados e, então, usar os resultados para auxiliar os usuários que estejam pesquisando por tópicos em particular. As grandes empresas nessa área são a Google, a Yahoo! e a Microsoft."

O desenvolvimento tecnológico também passou a possibilitar a existência de aplicativos e sites que possuem por objetivo a integração entre as pessoas pela internet, preferencialmente em tempo real, estes que foram denominados como "redes sociais". As pessoas perceberam a oportunidade de se manterem virtualmente próximas, bem como manterem contato mesmo com a distância física, por meio da tecnologia.

Em um primeiro momento, os crimes virtuais se resumiam a práticas ilícitas de usuários avançados e especialistas, denominados "crackers", que buscavam obter vantagens financeiras ou apenas testar suas habilidades por meio da invasão dos sistemas de grandes empresas e instituições. A partir da década de 90, com a popularização e barateamento do acesso à internet e do surgimento de novas tecnologias, já existe uma gama muito maior de crimes que são possíveis de serem cometidos no ambiente virtual, bem como é possível que qualquer indivíduo com conhecimentos básicos possa cometê-los.

Mesmo que trazendo um grande impacto positivo, à medida que a internet e esses novos mecanismos e softwares se popularizavam, tornando a navegação cada vez mais simplificada e agradável, bem como aprofundando e aprimorando as relações interpessoais, ficou também mais fácil cometer crimes anonimamente e à distância, até mesmo com certa garantia de impunidade, visto que é bastante difícil rastrear e coibir os delitos que podem ser cometidos na Web, considerando sua vastidão e complexidade.

Destaca-se o que dispõe o Superior Tribunal de Justiça sobre o assunto:

> "A internet é o espaço por excelência da liberdade, o que não significa dizer que seja um universo sem lei e infenso à responsabilidade pelos abusos que lá venham a ocorrer (STJ, REsp 1117633/RO, Rel. Ministro Herman Benjamin, Segunda Turma, julgado por unanimidade em 09/03/2010, DJe 26/03/2010)."

Se faz necessário que os crimes cibernéticos sejam devidamente definidos juridicamente, de acordo com suas especificidades, bem como devem ser elaborados dispositivos penais que sejam eficientes e adequados o suficiente às suas características especiais e únicas. O Código Penal e as demais normas gerais não suprem, de forma satisfatória, a grande lacuna legislativa existente no que tange às relações interpessoais na rede.

1.2 ACEPÇÃO DE CRIMES CIBERNÉTICOS

Antes de aprofundar mais no estudo do tema, é imperioso salientar a relevância e desenvolvimento das novas tecnologias, especialmente a internet e as redes sociais, pois a partir do momento em que a banda larga de acesso à internet se popularizou, a plataforma da web 2.0 passou a ser viável, além de possíveis as aplicações on-line participativas. Então, pode observar-se a proliferação das redes sociais on-line o tempo todo, sendo assim permitido a sua formação (GABRIEL, 2010, p. 83).

Assim, considerando que não é mais possível fazer a separação entre internet e fenômenos sociais, se faz necessária a adaptação aos novos meios de relações interpessoais informatizadas e às consequências decorrentes da nova era digital, como o surgimento de novas

formas de práticas de crimes. O direito brasileiro vem se desenvolvendo, lenta e tardiamente, no que tange à repreensão e punição desses delitos.

Por conseguinte, Ivette Senise Ferreira (2005, p. 261) classifica os crimes cibernéticos:

> "Atos dirigidos contra um sistema de informática, tendo como subespécies atos contra o computador e atos contra os dados ou programas de computador. Atos cometidos por intermédio de um sistema de informática e dentro deles incluídos infrações contra o patrimônio; as infrações contra a liberdade individual e as infrações contra a propriedade imaterial."

Neste ângulo, é possível concluir que os crimes cometidos pela internet trouxeram maior complexidade à aplicação do direito, especialmente para o direito penal. Cabe observar que surgiram novos crimes que somente podem ser cometidos por meio da rede e por dispositivos telemáticos e informáticos, os chamados crimes virtuais. Portanto, as inovações legislativas no que tange aos institutos penalizadores se mostraram extremamente necessárias, considerando o crescimento da rede e da conexão humana, que se dá de forma quase integral, às novas tecnologias.

Sobre o assunto, Tabosa *et. al.* (2007, p. 9) *c*ategoriza os crimes virtuais de acordo com sua finalidade:

> Categoria I: Insere delitos com a finalidade de reunir informações pessoais de forma a prejudicar de alguma maneira a vítima, conceituado de *phishing.* Por exemplo, a vítima inocentemente instala em seu computador algum tipo de vírus, o autor do crime tem a possibilidade de acessar os seus dados, unicamente, com a intenção de lhe prejudicar.
> -Categoria II: Abarca práticas de assédio e molestamento na internet, violência contra crianças, chantagem e intimidação. Por exemplo, o criminosos e insere em uma sala de bate-papo para interagir com a suposta vítima, estabelecendo uma relação de confiança, visto a facilidade de diálogo entre ambas e a "inocência" da mesma para concretizar relações afetivas. Após a consolidação da relação de confiança, os criminosos manipulam as vítimas de forma a praticarem atos que podem envolver a automutilação.

O estudo dos crimes cibernéticos, analisando desde a forma que ocorrem até suas características únicas, é primordial para a criação de dispositivos penais eficientes e para que seja possível buscar formas de reduzir ou coibir a sua incidência, o quanto for possível. Uma

das etapas mais importantes dessa análise é também a categorização desses crimes entre próprios e impróprios.

Nessa seara, Damásio Evangelista de Jesus (*apud* CARNEIRO, 2012, [n.p.]) afirma que:

> Crimes eletrônicos puros ou próprios são aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado.

Ainda não se trata de uma tarefa simples a definição desses crimes, que vão desde *spams* até exposição de informações sigilosas ou pessoais, transferência de vírus ou mesmo a invasão de dispositivos. Esporadicamente vão surgindo inovações no que tange a esses delitos. Entretanto, os crimes cibernéticos impróprios (ou impuros) ainda são preponderantes, pois consistem em atingir os meios jurídicos já tipificados utilizando-se de um instrumento tecnológico, como computador ou celular, por meio da rede informática, não permanecendo necessariamente na esfera virtual.

Nesta seara, também define Damásio de Jesus (apud CARNEIRO, 2012, [n.p.]) que:

> Já os crimes eletrônicos impuros ou impróprios são os que o agente se vale do computador como sendo um meio de produção de resultado naturalístico, onde ofenda o mundo físico ou o espaço "real", ameaçando ou vindo a lesar outros bens, não computacionais ou diferentes da informática.

Sendo assim, após se definir os crimes cibernéticos e sua forma de execução, é possível o uso de analogia para aplicação do Código Penal, enquanto inexistente tipificação mais específica. Os crimes cibernéticos impróprios são mais facilmente observados e punidos, por se assemelhar a crimes já tipificados na norma penalizadora.

O ordenamento jurídico brasileiro ainda carece, no entanto, de normas mais específicas para coibir tais práticas, especialmente os crimes cibernéticos próprios. Mesmo que as normas específicas sejam estabelecidas, ainda será necessário percorrer um longo caminho até a efetiva dissuasão dos criminosos em potencial, visto a facilidade e agilidade com que esses crimes podem ser cometidos, principalmente de forma anônima. Acerca do tema, dispõe Corrêa:

> (...) Talvez o pequeno número de casos submetidos à polícia e a nossos tribunais faça com que a habilidade técnica para "fechar o cerco" a tais "crimes" deixe a desejar. Isso é preocupante, pois, como demonstrado anteriormente, a tendência é o aumento qualitativo e quantitativo de tais ilícitos. (CORRÊA, 2010, p.91).

O Brasil, apenas a partir de poucas décadas atrás, passou a preocupar-se com as consequências do acelerado desenvolvimento tecnológico e informático, com a promulgação de leis como a "Lei Carolina Dieckmann" e o "Marco Civil da Internet", que representaram referências para o aprimoramento normativo que já se fazia extremamente necessário. Ou seja, é visível e latente a necessidade de evolução legislativa no que tange a punibilidade dos crimes virtuais, por meio da criação de leis específicas e efetivas, a fim de combater os delitos no âmbito da rede internacional de computadores.

Cabe destacar que há também uma crescente incidência de crimes transnacionais, que são aqueles que podem atingir diversas nações simultaneamente, não se limitando às fronteiras nacionais, sendo necessário um esforço internacional para combatê-los, como Ivette Senise Ferreira (2008, p. 213) expõe:

> Já se deu a internacionalização da criminalidade informática, devido à mobilidade dos dados nas redes de computadores, facilitando os crimes cometidos à distância. Diante desse quadro, é indispensável que os países do globo harmonizem suas normas penais, para prevenção e repressão eficientes.

O Superior Tribunal de Justiça (2008, online), por meio de seu informativo eletrônico, já se manifestou quanto à inexistência de legislação específica que tipifique os crimes cibernéticos, dissertando acerca da necessidade latente dessas inovações legislativas, bem como sobre as dificuldades enfrentadas pelos aplicadores do direito:

> "Na ausência de uma legislação específica para crimes eletrônicos, os tribunais brasileiros estão enfrentando e punindo internautas, crakers e hackers que utilizam a rede mundial de computadores como instrumento para a prática de crimes. Grande parte dos magistrados, advogados e consultores jurídicos considera que cerca de 95% dos delitos cometidos eletronicamente já estão tipificados no Código Penal brasileiro por caracterizar crimes comuns praticados por meio da internet. Os outros 5% para os quais faltaria enquadramento jurídico abrangem transgressões que só existem no mundo virtual, como a distribuição de vírus eletrônico, cavalos-de-tróia e worm (verme, em português)".

Por isso, para a aplicação do direito de maneira satisfatória no que tange aos crimes virtuais, não basta que o magistrado venha a realizar uma interpretação extensiva ou analógica no caso concreto, sendo necessário que exista uma legislação específica que possibilite o enquadramento jurídico adequado dessas transgressões, que só ocorrem no âmbito do ciberespaço.

1.3 PRINCÍPIOS DO DIREITO PENAL BRASILEIRO E O CYBERCRIME

Quando se fala em *cybercrimes,* a privacidade é o primeiro ponto que deve vir a ser destacado, tanto que na literatura o primeiro tipo de lei criada para amparar o usuário da rede surgiu em 2012. No entanto, antes dessa data, outras leis já haviam sido criadas para que fosse aumentada paliativamente a segurança sobre outros tipos de crimes, que foram se expandindo juntamente com a internet, cabendo destacar a Lei nº 11.829/2008, que objetivou trazer proteção aos direitos das crianças e adolescentes, especialmente no que tange à posse e aquisição de material pornográfico e demais condutas relacionadas à pedofilia no ambiente virtual.

Os principais passos para atualização penal, no que diz respeito aos crimes informáticos, remetem à compreensão de como são definidos esses crimes e como se apresentam, conforme podemos observar.

De acordo com esse contexto, é de fundamental importância que seja apurado o exato momento que tenha ocorrido o fato típico, de modo que seja corretamente aplicada a norma penal, já que os meios informáticos trazem uma pequena dissociação temporal, possibilitando até mesmo a programação de um delito. Portanto, a ação poderia acontecer em tempo real ou ficto, dependendo da vontade do agente.

Assim, para efeito penal, no que tange ao tempo do crime, considera-se válida como referência a ação inicial que programou a execução, ainda que essa aconteça em momento posterior, ou seja, aplica-se a teoria da atividade. Referente ao tema, dispõe o Artigo 4º do Código Penal, que: “considera-se praticado o crime no momento da ação ou omissão, ainda que outro seja o momento do resultado”.

Sobre o lugar do crime, por outro lado, adotou-se como regra o princípio da territorialidade, porém, a dificuldade enfrentada é que o meio virtual não possui espaço físico delimitado, gerando assim um acesso dinâmico amplo, onde a concepção de território como espaço físico dá lugar para o virtual, vindo a transcender os limites territoriais e ensejando na aplicação do princípio da extraterritorialidade para ser resolvido o conflito, em diversos casos. Os referidos princípios estão dispostos nos artigos 5º e 7º do Código Penal.

Cabe destacar que o Brasil aderiu à Convenção sobre o Cibercrime, também conhecida como Convenção de Budapeste, que nada mais é que um tratado internacional do Conselho da Europa que buscava dispor quanto as formas de combate aos crimes praticados no âmbito virtual, em especial os delitos de caráter transnacional, por meio da tentativa de adoção de uma política criminal comum, o que não foi suficientemente efetivo na prática. Acerca do tema, dispõe o artigo 22 da referida Convenção:

> Cada parte adotará as medidas legislativas e outras que se revelem necessárias para estabelecer à competência relativamente a qualquer infração penal definida em conformidade com os artigos 2º *a* 11º da presente Convenção, sempre que a infração seja cometida:
> a) no seu território;
> b) a bordo de um navio;
> c) a bordo de aeronave matriculada nessa parte e segundo as suas leis; ou
> d) por um dos seus cidadãos nacionais, se a infração for punível criminalmente onde foi cometida ou se a infração não for de competência territorial de nenhum Estado (BUDAPESTE, 2001).

Já no que diz respeito à materialidade, o crime digital é um ilícito que deixa vestígios, sendo imposta a perícia, nos termos do artigo 158 do Código de Processo Penal. O perito possui obrigação de esclarecer ao magistrado, todas as circunstâncias necessárias para demonstrar a ocorrência do crime, além da comprovação de determinada autoria.

Ressalta-se que os crimes cometidos pela internet seguem a regra geral de competência para julgamento, que se encontra disposta no Código de Processo Penal em seu artigo 69, *in verbis:*

> Art. 69. Determinará a competência jurisdicional:
> I - o lugar da infração:

> II - o domicílio ou residência do réu;
> III - a natureza da infração;
> IV - a distribuição;
> V - a conexão ou continência;
> VI - a prevenção;
> VII - a prerrogativa de função.

Por esses motivos, os crimes de possível constatação de localidade serão processados no foro em que foi produzido o resultado.

2 DOS DIREITOS À PRIVACIDADE E INTIMIDADE NA INTERNET

Muitos países têm leis projetadas para proteger a privacidade, e toda organização que coleta e armazena informações sobre indivíduos é legalmente obrigada a adotar políticas que estejam em conformidade com a legislação de privacidade local. De acordo o Alves (2006), a armazenagem de dados pode ser considerada a espinha dorsal de muitos aplicativos atualmente. Portanto, os ataques aos bancos de dados também estão aumentando, e essas são formas muito perigosas e possivelmente danosas de investida, pois revelam dados sensíveis e privados importantes ao invasor.

No Brasil, o primeiro caso de grande relevância e notoriedade foi da atriz Carolina Dieckmann, ocorrido no ano de 2011, ocasião em que um hacker invadiu o seu computador pessoal e roubou diversas fotos intimas, bem como ameaçou divulgar as fotos caso não recebesse a recompensa solicitada. Como consequência desse fato, ainda no ano de 2011, foi apresentado o projeto de lei para tipificar o crime de invasão de dispositivo telemático, tendo sido aprovado em dezembro de 2012. O ponto de maior relevância da nova norma foi a inclusão de novos tipos penais incriminadores ao Código Penal, os artigos 154-A e 154-B:

> 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.
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos.

Esses artigos tratam do comportamento de acesso forçado à dispositivos telemáticos sem a autorização dos proprietários, geralmente com intuito malicioso. Trata-se de um crime formal, pois não importa se o resultado de fato é alcançado, bastando a tentativa de invasão para restar tipificado o delito. Uma das formas mais comuns de prática do crime de invasão de dispositivos é o *Phishing*, conceito em Inglês que significa “pescar”. Trata-se de um golpe comum na internet, que por meio de e-mail, site ou mensagem de texto, o criminoso “pesca” a

vítima com o objetivo de roubar informações pessoais. A vítima apenas precisa clicar em um *link* ou arquivo e preencher com seus dados para ser invadido.

Os assuntos das mensagens e e-mails são bem diversificados, onde os invasores fingem ser organizações ou instituições confiáveis, como Correios, bancos ou sites de compras, de modo a convencer a vítima a fazer algum procedimento ou preencher algum dado sensível. Caso a vítima confie e realize o procedimento, o dispositivo é invadido ou os dados são roubados.

O golpe desse tipo de maior valor aconteceu em 2013, quando um *hacker* chamado Evaldas Rimasuaskas falsificou e-mails corporativos e os enviou para o Google e Facebook, fazendo com que essas empresas transferissem dinheiro para suas contas bancárias na Europa. O plano funcionou por cerca de dois anos e o criminoso conseguiu roubar 100 milhões de dólares.

As três principais variações de *Phishing* são:

- Smishing é realizado por mensagens de texto e SMS.
- Vishing por meio de chamadas telefônicas.
- Pharming é acontece quando um código malicioso é instalado para redirecionar a vítima para sites falsos.

O código penal faz menção a respeito da violação do direito à privacidade nos seguintes artigos, *in verbis*:

> Art. 153 - Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem:
> Art. 151 - Devassar indevidamente o conteúdo de correspondência fechada, dirigida a outrem:
> II - Quem indevidamente divulga, transmite a outrem ou utiliza abusivamente comunicação telegráfica ou radioelétrica dirigida a terceiro, ou conversação telefônica entre outras pessoas;

Esses artigos dispõem sobre a divulgação de conteúdo particular ou correspondência confidencial, da qual a exposição cause danos a terceiros, sendo admissível a tentativa. Maria Helena Diniz (2007) explicita que, quando ocorre a violação da intimidade e da privacidade, a

vítima deverá ser protegida constitucionalmente, caso seus arquivos pessoais sejam compartilhados na internet:

> A intimidade é a zona espiritual íntima e reservada de uma pessoa ou de um grupo de indivíduos, constituindo um direito da personalidade, daí o interesse jurídico pelo respeito à esfera privada. Desse modo, o autor da intrusão arbitrária à intimidade alheia deverá pagar uma indenização pecuniária, fixada pelo órgão judicante de acordo com as circunstâncias, para reparar dano moral ou patrimonial que causou. Além disso, deverá o magistrado ordenar medida que obrigue o ofensor a cessar suas ingerências na intimidade alheia, se estas ainda continuarem e, se possível, deverá exigir o restabelecimento da situação anterior à violação, a expensas do lesante, como, p. ex., a destruição da coisa produzida pelo atentado à intimidade. (DINIZ, 2007, p. 160).

Portanto, conclui-se que a indenização somente irá assumir caráter pedagógico ou punitivo de forma acessória, eis que sobre a responsabilização no âmbito civil deve prevalecer a função indenizatória e reparadora, onde o sujeito que causou o dano deverá ressarcir o indivíduo lesado. (DINIZ, 2007, p. 130)

Em muitos casos de violação da intimidade, entretanto, existe a dificuldade em avaliar o valor que será pago à título de indenização pelo dano moral sofrido. Embora a proteção à intimidade e à vida privada esteja prevista na Constituição Federal, destaca-se o Marco Civil da Internet como sendo a primeira lei infraconstitucional a regulamentar o tema. Esclarece ser cabível indenização por dano moral ou material comprovado, automaticamente, decorrente da violação dessas proteções na internet. (DAMÁSIO, 2014)

Pode-se entender o direito à intimidade como sendo o direito pessoal de garantir que terceiros não venham a ter conhecimento de coisas ou mesmo situações que o indivíduo não tenha vontade, interesse ou mesmo a necessidade de expor, sendo faculdade do mesmo a escolha de proceder o compartilhamento ou não dessas informações, devendo possuir proteção para tanto.

Não se pode trazer a intimidade à tona para a coletividade, pois segundo Arendt (2005, p. 62), seus assuntos são iluminados à meia-luz, onde se deve, na sua maioria das vezes, serem escondidas da visão dos indivíduos. Tal ideia deriva da noção de percepção da realidade, pois os indivíduos necessitam de boa aparência para que seja mantida uma relação saudável com o

público. Vários acontecimentos do cotidiano não poderiam suportar a exposição, por isso, mantém-se em segredo como garantia da uma convivência pacífica na sociedade.

Existe ainda quem defenda que o direito à intimidade é um prolongamento de outros direito da personalidade, porém não se pode assim entender, pois o mesmo faz parte de uma categoria que é autônoma, não se confundindo com os outros direitos, visto que em um mesmo ato pode-se ferir concomitantemente os direitos ao sigilo, à honra, à vida privada e à intimidade.

Sobre o assunto, afirma Manoel Jorge e Silva Neto (2013, p.733):

> "Se a Constituição Federal assinala serem invioláveis a intimidade, a vida privada, a hora e a imagem das pessoas, é correto visualizar a autonomia de cada qual, especialmente se o propósito está voltado à concepção de um catálogo de direitos fundamentais apto a cumprir a meta desenhada: a defesa da cidadania e do Estado Democrático de Direito".

Pode-se inferir que a Constituição Federal de 1988 não fez a separação dos institutos por simples vontade, mas sim, para que não fosse admitido que existisse duas terminologias para um mesmo direito individual.

No que tange aos direitos à intimidade e à vida privada, Sílvio Romero Beltrão possui a seguinte visão:

> A intimidade e a vida privada são erigidas na Constituição como valores humanos, na condição de direito individual e para tanto em defesa deste direito fundamental, nos preocupamos em preservá-las do conhecimento alheio. Nossos erros, nossas imperfeições e até mesmo nossas virtudes não devem estar obrigatoriamente expostas ao domínio público, pois, interesses variados podem forçar-nos a ocultar determinados fatos do conhecimento de outras pessoas. Vários exemplos poderiam ser citados, como interesses exclusivos de ordem privada e intima, a justificar a sua preservação do conhecimento alheio. Em tais situações, terceiros desautorizados não podem violar os segredos e reservas da pessoa, pois, certamente causariam transtornos e danos irreparáveis. (BELTRÃO, 2017, p. 1)

No que se refere ao direito à intimidade, para Pedro Frederico Caldas (1997, p. 47), além das características que são comuns aos direitos da personalidade, tem outra que é própria do mesmo, a que se refere à não exposição ao conhecimento de terceiros de algum elemento particular da esfera que é reservada ao titular. No Brasil, é perceptível que não existe um

conceito de intimidade que é aceito por unanimidade entre os doutrinadores. Existem, portanto, conceitos abertos onde a interpretação depende de cada magistrado, podendo sofrer alteração conforme a pessoa e o local.

Sobre as legislações existentes, conforme já dito, destaca-se o dispositivo presente na Constituição Federal de 1988, artigo 5º, inciso X. Existem também leis esparsas, como é o caso do Código Civil em seu artigo 21, que traz a inviolabilidade da vida privada natural, onde abrange-se a intimidade, e o magistrado, se o interessado requerer, poderá adotar as providências que forem necessárias para frustrar eventual violação.

Também no Código Civil se tem outros dispositivos, que mesmo que de forma implícita, buscam resguardar os aspectos particulares da vida das pessoas, destacando-se o artigo 144 onde existe matéria de prova e proteção do direito ao segredo que for resultado de estado ou mesmo profissão, quando as pessoas precisam guardar segredos de fatos que aconteceram e não estão obrigadas a depor perante o magistrado. Também cumpre evidenciar os artigos 573 a 576, os quais tratam da colocação de janelas, eirado, terraços ou varandas, devendo sempre respeitar algum espaço do imóvel do vizinho, bem como questões relativas à sua vida privada.

Nessa seara, também cabe salientar a proteção presente no Código de Processo Civil, o qual detém artigos que possuem relação com a tutela dos direitos ao respeito e à privacidade, bem como também à intimidade. Podemos exemplificar o artigo 404, que diz respeito aos casos da negativa de exibição em juízo de documento ou qualquer outro fato que possua relação com os negócios da vida da própria família e que viole o dever de proteção à honra.

Os referidos institutos são fundamentais, abrangendo infinitas interpretações. Existe uma necessidade cada vez maior de regulamentar em relação ao tema intimidade, principalmente no ambiente virtual, pois constantemente surgem novas questões que não estão abrangidas de maneira específica e integral pelo ordenamento jurídico.

Também é mencionado na Constituição Federal de 1988 que "(...) é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei penal estabelecer para fins de investigação criminal ou instrução processual penal".

Dessa forma, pode-se constatar que, a Constituição visa proteger a liberdade de expressão, em todas as suas modalidades, e a privacidade em todos os seus níveis de densidade, sendo uma exigência democrática que está ligada à proteção dos direitos humanos e fundamentais albergados na Carta Magna. Entretanto, se faz necessária a elaboração de dispositivos que regulamentem de maneira mais específica e detalhada as proteções que se busca garantir.

Além disso, pode-se conceituar acerca de outros tipos de crimes decorrentes da informatização. Para que se possa contextualizar sobre os *Ransomwares,* primeiramente deve-se entender do que se trata um *malware*. Os *malwares* são *softwares* maliciosos, criados com o único propósito de causar dano a quem o contrai. São eles que danificam dispositivos, roubam dados, bloqueiam sistemas, entre outras finalidades.

No caso dos *Ransomwares,* que é a junção de *ransom* (resgate, em português) e *software* (programa de computador), são malwares que infectam os dispositivos e se utilizam da criptografia para restringir o acesso aos dados do sistema pelo usuário. A criptografia é a conversão de dados de um formato legível pelo dispositivo em um formato codificado (não legível). Os dados criptografados só podem ser lidos ou processados depois de serem descriptografados, nesse caso, pelo invasor após recebimento de "resgate" pago pela vítima. Os cibercriminosos ameaçam expor ou apagar os dados confidenciais e importantes da vítima e, para que o acesso seja restabelecido, é concretizada uma extorsão, na maioria das vezes, paga por criptomoedas (dinheiro digital), como o Bitcoin.

Esse pagamento é feito por essas moedas virtuais pelo fato de que são praticamente irrastreáveis, mantendo assim, anônima a identidade do cibercriminoso. O número de ataques de *ransomware* vem aumentando com uma alta frequência no decorrer dos anos, sendo os maiores alvos grandes empresas e instituições, visto que podem pagar um alto valor de resgate e possuem dados extremamente sensíveis. Esse tipo de crime rendeu pelo menos 350 milhões de dólares (quase 1,9 bilhão de reais, em conversão direta) em 2020 — um aumento de 311 por cento de volume se comparado a 2019 (Chainalysis, 2021). Caso as empresas continuem não dando a atenção necessária para a área de segurança da informação, a expectativa é que esse número não pare de crescer nos próximos anos.

Nas últimas décadas, a informática desenvolveu-se demasiadamente, e umas das implicações desse desenvolvimento exagerado é que deixou de representar mero instrumento que tinha o propósito de potencializar os processos administrativos, e se transformou em uma ferramenta inteligente para a indústria em geral, a administração e até mesmo as forças armadas. Com isso, grandes empresas especializadas em segurança da informação, tais como a *Kaspersky, Akamai, Sophos, Ecoit, Norton, Malwarebytes, McAfee*, dentre outras, vem evoluindo seus sistemas de gerenciamento a vulnerabilidades, para melhor identificação e rastreio de *malwares* com o intuito de identificar e destruí-los. (KASPERSKY, 2021)

Quanto maior for o tráfego de informações em redes de telecomunicações e maior a quantidade de informação armazenada em meios computacionais, maior será a necessidade de empresas, governos e até de pessoas físicas de se protegerem contra essa nova ameaça que está crescendo proporcionalmente ao desenvolvimento da informática.

2.1 MARCO CIVIL DA INTERNET: PRINCÍPIOS DA REDE NO BRASIL

No Brasil, durante o ano de 1995, foi criado um órgão consultivo relacionado à coordenação e integração de todas as atividades ligadas à internet no Brasil denominado Comitê Gestor da Internet – CGI. Por meio do decreto no 4.829/2003, esse órgão foi reestruturado. Ele possui caráter consultivo e também estabelece as diretrizes estratégicas no que tange ao desenvolvimento e uso da Internet no Brasil.

Conforme aponta Machado (2002), tem em suas principais atribuições criar e discutir diretrizes ligadas a uma visão estratégica com relação ao uso e desenvolvimento da internet no âmbito nacional, bem como promover uma relação entre governo e a sociedade no tocante ao desenvolvimento de políticas, mecanismos adequados ligados à governança da internet no Brasil e discussão de aspectos que aliem a parte técnica da rede, como sua infraestrutura, e o tratamento jurídico das questões relacionadas à internet. Dentre uma das atividades realizadas pelo CGI estão as reuniões ordinárias, que buscam tratar e deliberar sobre assuntos relacionados à governança e ao desenvolvimento da internet no país.

No ano de 2009, em uma dessas reuniões ordinárias, por meio da Resolução 003/2009, com o antecedente debate e discussão, foram criados e estabelecidos dez princípios relativos à governança da internet no Brasil, e esses princípios ficaram conhecidos popularmente como “O decálogo da internet”. A criação do decálogo da internet antecedeu o surgimento do próprio Marco Civil da Internet, porém criou uma base sólida para discussão do Projeto de Lei 2.126/2011, que mais tarde deu origem à Lei 12.965/2014.

A finalidade desses princípios foi servir de base para o entendimento de questões basilares relativas à internet no Brasil, como, por exemplo, a liberdade de expressão, a privacidade e a proteção de dados pessoais. Os princípios que compõem o decálogo da internet são: liberdade, privacidade e direitos humanos, governança democrática e colaborativa, universalidade, diversidade, inovação, neutralidade da rede, inimputabilidade da rede, funcionalidade, segurança e estabilidade, padronização e interoperabilidade, ambiente legal e regulatórios.

Esses princípios servem de vetores interpretativos para o entendimento do conjunto de preceitos que estão contidos no bojo do ordenamento jurídico brasileiro e que tratam das relações dentro da internet, o qual se destaca o Marco Civil, que foi a primeira lei específica a tratar das especificidades necessárias para compreensão do ambiente que representa o ciberespaço. Segundo Machado (2002), o decálogo da internet estabelece princípios basilares para o uso da rede mundial de computadores no Brasil, e se constituiu como uma importante iniciativa jurídica. Essa iniciativa foi ao encontro da necessidade de regulação efetiva na internet, no sentido de estabelecer normas e parâmetros no ordenamento jurídico brasileiro que tratem das relações e crimes no âmbito do ambiente virtual.

O CGI se utilizava desses princípios, desde o ano de 2009, como norte para suas decisões e ações, segundo preceitos fundamentais. Os princípios perduram, mesmo que com sensível perda de efetividade e força, tendo influenciado diretamente na elaboração e desenvolvimento do Marco Civil da Internet e na LGPD. A maior problemática gira em torno da crescente evolução e transformação da internet, podendo os princípios não mais atenderem satisfatoriamente às necessidades da “nova internet” em pouco tempo.

Discorre Possebon (2019, p. 44) acerca da rápida mutação da rede e da possibilidade de que esses princípios se tornem obsoletos em poucos anos:

> De qualquer forma, os princípios do CGI foram essenciais para o ambiente normativo da Internet brasileira e são ainda atuais. A questão é se serão suficientes para os próximos 10 anos, em que o papel dos algoritmos, da inteligência artificial, de grandes conglomerados tecnológicos e de uma nova geopolítica global são o pano de fundo para uma nova Internet para humanos e coisas.

Então, se deu especial atenção ao direito à privacidade, entendido aqui, sob o ponto de vista do direito civil, como sendo o direito de isolar-se do contato com outras pessoas, bem como o direito de impedir que terceiros tenham acesso a informações acerca de sua pessoa (AMARAL, 2008, p.306). Isso se encontra previsto nos incisos I, II, III, VII e VIII do art.7º, ao elencarem-se como direitos dos usuários de internet a inviolabilidade da intimidade e da vida privada, a preservação do sigilo das comunicações privadas pela rede, transmitidas ou armazenadas, bem como o não fornecimento de dados pessoais coletados pela internet a terceiros sem prévio consentimento do usuário, além de estabelecer o dever de passar para os usuários informações sobre a coleta de dados sobre si, quando existir uma justificativa para tal fato.

Da mesma maneira, o artigo 10 do Marco Civil da Internet estabeleceu que a guarda e disponibilização dos registros de conexão e de acesso a aplicações de internet devem ser realizadas com respeito à intimidade, vida privada, honra e imagem das pessoas direta ou indiretamente envolvidas. Já os artigos 14 e 16, dispuseram que o provedor de conexão à internet não pode guardar registros de acesso a aplicações da internet, bem como não pode guardar os registros de acesso sem prévio consentimento do usuário, assim como dos dados pessoais desnecessários à finalidade para a qual se deu consentimento. Já no artigo 9°, §3º, proíbe-se que os provedores de conexão à internet, gratuitos ou onerosos, ou os responsáveis pela transmissão, comutação e roteamento de dados, realizem bloqueios, filtros ou análises de conteúdo dos pacotes de dados.

O Marco Civil da Internet disciplinou a atuação do Poder Público em se tratando do desenvolvimento da internet no Brasil. Com isso, previu-se nos artigos 24 e 25, o estabelecimento de mecanismos de governança multiparticipativa, onde foram envolvidos o

governo, as empresas, a sociedade civil e a comunidade acadêmica, à racionalização da gestão, expansão e utilização da internet no Brasil, especialmente, na implantação de serviços de governo eletrônicos e de serviços públicos, na adoção preferencial de tecnologias, padrões e formatos abertos e livres, na publicidade de dados e informações públicos na internet e, sobretudo, no estímulo à implantação de centros de armazenamento, gerenciamento e disseminação de dados no Brasil.

Por fim, no caso dos artigos 26 e 27, tratam do uso da internet como ferramenta para o exercício da cidadania, promoção da cultura e desenvolvimento tecnológico, sobretudo para a promoção da inclusão digital, redução de desigualdades sociais e fomento à produção e circulação de conteúdo nacional. Ademais, desistiu-se da ideia de implantação compulsória de datacenters de aplicações de internet no Brasil, ao apenas estabelecer, no artigo 24, VII, o estímulo à implementação desses no Brasil, mas não a obrigatoriedade.

2.2 PROTEÇÃO DE DADOS PESSOAIS NA INTERNET

Preliminarmente, cumpre destacar que a preocupação com a transmissão e segurança dos dados deve ser algo determinante nas instituições, órgãos, empresas, e principalmente, nas mídias sociais. Um fator importante neste aspecto foi a origem da Lei n° 13.709/2018, que foi concebida a partir da grande repercussão referente ao vazamento dos dados gerados pela rede social Facebook. E agora, com o advento desse dispositivo, isso é inadmissível, como estabelecido na seção da segurança e do sigilo de dados, nos artigos 46, 47, 48, em seus incisos e parágrafos, conforme a seguir:

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito.
> § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.

> § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.
> Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.
> Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
> § 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:
> I - a descrição da natureza dos dados pessoais afetados;
> II - as informações sobre os titulares envolvidos;
> III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
> IV - os riscos relacionados ao incidente;
> V - os motivos da demora, no caso de a comunicação não ter sido imediata; e
> VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.
> § 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:
> I - ampla divulgação do fato em meios de comunicação; e
> II - medidas para reverter ou mitigar os efeitos do incidente.
> § 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.
> Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

Dessa forma, pode-se concluir, a respeito da segurança e sigilo das informações das pessoas, que os agentes responsáveis pelas mídias sociais devem adotar medidas de segurança, técnicas e administrativas, que possuem o intuito de fornecer proteção aos dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

A segurança de dados é utilizada para manter o sigilo e controle das ações que serão efetuadas no conteúdo guardado pelo interessado, e por isso, organizações também estão buscando se capacitar e aperfeiçoar em instrumentos e recursos que possam garantir a segurança de seus dados. A tecnologia pode ser a melhor ferramenta para gerar recursos de segurança. Com isso, empresas passaram a adotar metodologias práticas para concretizar a referida proteção. (ALVES, 2006)

Com o grande avanço da internet, os direitos à intimidade e privacidade tem sido constantemente violados, pessoas acabam por ficar mais vulneráveis, e algo que deve ser extremamente pessoal acaba por ser invadido, ou até mesmo exposto, causando problemas para a vítima. Independentemente de fazer parte do grupo de pessoas sem grande conhecimento sobre o ambiente virtual ou do grupo de usuários mais experientes, ninguém está totalmente livre e seguro contra usuários e programas maliciosos.

Segundo Gustavo Alves (2006), a segurança de dados visa proteger a informação de forma a garantir continuidade dos negócios, minimizando os danos e maximizando o retorno dos investimentos e as oportunidades de negócios. Dados e negócios podem andar juntos e gerando grande capital. Bancos de dados podem guardar informações cruciais para o funcionamento e desenvolvimento de uma empresa, tornando-se um grande alvo de ataques maliciosos com intuito de roubar dados importantes.

Para um profissional visualizar e manusear um banco de dados, é necessário se ter uma permissão para acessar a devida informação. Elmasri e Navathe (2011) exemplificam o caso em que um administrador, que deve ter a permissão para alterar as informações de alunos, pode acabar usando esse privilégio para atualizar as notas dos mesmos sem a permissão do instrutor. Conclui-se, portanto, que uma permissão de grande responsabilidade não pode, de forma alguma, ser utilizada de forma maliciosa ou indevida. Para Silberschatz (1999), as regras de integridade devem fornecer a garantia de que mudanças feitas no banco de dados por usuários autorizados não resultem em perda da consistência dos dados. Assim, as regras de integridade protegem o banco de dados de danos que podem ser originados de forma acidental ou intencional.

A segurança de modo geral é importante, onde o profissional que recebe acesso a dados restritos é responsável por sua segurança, devendo verificar e identificar brechas que apontam falhas e erros de segurança, bem como todo acesso deverá ser registrado para controle e verificação.

Para Machado (2004), para que o dado fique protegido do uso indevido de qualquer usuário, recursos como a linguagem SQL podem permitir que se defina os privilégios que cada

um pode ter em relação às tabelas criadas no banco de dados. Dessa forma, os privilégios garantem sua segurança e integridade, bem como a responsabilidade de cada usuário sobre seus dados específicos.

Como visto anteriormente, um acesso restrito usado de maneira maliciosa pode trazer um grande risco. Segundo Sêmola (2003 p. 67), “risco é a probabilidade de ameaças explorarem vulnerabilidades, provocando perdas de confidencialidade, integridade e/ou disponibilidade, causando, possivelmente, impactos nos negócios”.

Além da incumbência de preservar e proteger os dados para o bom funcionamento das organizações, projetistas de bancos de dados possuem a responsabilidade de proteger a privacidade das pessoas sobre as quais os dados são mantidos. Privacidade pode ser definido como direito das pessoas de ter algum controle sobre suas próprias informações. (SÊMOLA, 2003)

A Lei n° 13.709/2018, que regula o tratamento de dados pessoais no Brasil, tem como premissa assegurar o respeito à vida privada em relação aos fluxos comunitários de dados pessoais. Como já dito, seu objetivo é proteger "os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (BRASIL, 2018), inclusive nos meios digitais, não excluindo o meio físico, como dados em documentos, currículos, formulários e holerites.

Liminarmente, o art. 1º da Lei nº 13.709 de 14 de agosto de 2018 – Lei Geral de Proteção de Dados, estabelece que:

> 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 (BRASIL, 2018)

Popularmente conhecida como LGPD, dispõe em seu artigo 2º os fundamentos que busca disciplinar, quais sejam: a proteção de dados pessoais no respeito a privacidade, a autodeterminação informativa, a liberdade de expressão, de informação, de comunicação e de opinião, a inviolabilidade da intimidade, da honra e da imagem, o desenvolvimento econômico

e tecnológico e na inovação, a livre iniciativa, a livre concorrência e a defesa do consumidor e essencialmente os direitos humanos.

O titular dos dados pessoais é a pessoa natural (física) a quem se referem os dados pessoais que são objeto de tratamento, observando-se que as pessoas jurídicas não são incluídas. O artigo 5° da LGPD define, também, o que é dado pessoal, sendo a “informação relacionada à pessoa natural identificada ou identificável” (BRASIL, 2018) e dado sensível como “dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural” (BRASIL, 2018).

A referida lei não será aplicada no tratamento de dados pessoais em virtude de pessoa natural para fins exclusivamente particulares e não econômicos, jornalísticos, artísticos ou acadêmicos. No entanto, torna-se efetiva para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais. (BRASIL, 2018)

Os princípios norteadores desta lei estão inseridos em seu artigo 6°, além da boa fé, o princípio da finalidade descrito na própria Lei como a "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades" (BRASIL, 2018), bem como o princípio da adequação, definido como a “compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento” (BRASIL, 2018), ou seja, os dados devem ser adequados, pertinentes e não excessivos em relação a seus fins.

Tem-se também o princípio da necessidade, descrito como a "limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados" (BRASIL, 2018), o princípio do livre acesso, descrito como a "garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais" (BRASIL, 2018), bem como o princípio da qualidade dos dados, descrito como a "garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento"

(BRASIL, 2018). Nesse último, é possível compreender que as informações incorretas devem ser corrigidas, as obsoletas ou impertinentes devem ser suprimidas, assim como ainda é possível que o proprietário dos dados solicite eventuais acréscimos e atualizações para manter a exatidão dos dados, buscando prover o melhor direito do titular por manter as informações sempre condizentes com a realidade.

Encontra-se descrito, ainda, o princípio da transparência, que dá o direito ao titular de conhecimento da existência de um arquivo de dados, o princípio da segurança, que exige "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" (BRASIL, 2018), o princípio da prevenção, traduzido na "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais" (BRASIL, 2018), assim como o princípio da não discriminação, que consiste na "impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos (BRASIL, 2018), devendo os dados devem ser tratados para os propósitos determinados e que devem ser informados ao titular.

Por fim, dispõe sobre o princípio da prestação de contas, encontrado na Lei como "demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas" (BRASIL, 2018).

No que diz respeito ao tratamento e utilização de dados pessoais, entende-se que poderão ser realizados desde que haja consentimento do titular, bem como essa manifestação de vontade deve ser expressa por escrito ou outro meio que evidencie a concordância do indivíduo.

É assegurada, a toda pessoa natural, a titularidade de seus dados pessoais, garantido seus direitos fundamentais e assegurando a confirmação da existência de tratamento, acesso aos dados, correção de dados incompletos, inexistentes ou desatualizados, anonimização, bloqueio ou eliminação de dados desnecessários (BRASIL, 2018).

Para regular a LGPD, foi criada através da Medida Provisória nº 869/2018, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal que é

submetida ao regime autárquico especial vinculado à Presidência da República. A ANPD é composta por Conselho Diretor, órgão máximo de direção, assim como por Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, Corregedoria, Ouvidoria, órgão de assessoramento jurídico próprio e unidades administrativas, bem como unidades especializadas necessárias à aplicação do disposto pela Lei (Medida Provisória nº 869/2018).

No dia 29 de abril de 2020, foi publicada a Medida provisória nº 959/2020, que adiou a entrada em vigor da LGPD para 03 de maio de 2021. A prorrogação foi motivada em virtude da Pandemia do Coronavírus no intuito de que fossem postergadas as multas e sanções às entidades.

Segundo Mance (1999), através do fenômeno da internet passou a surgir a criação das redes sociais, que utilizam as tecnologias das informações e das comunicações para se articular e auto organizar, o que passou a tomar dimensões globais. Com o avanço das mídias sociais, que repercute de forma internacional através das trocas de informações e estabelecimento de comunicações, trata-se de um movimento descentralizado, com formação de redes. Pode-se compreender que essa rede tem o seu funcionamento de forma aberta e dinâmica, assim como com auto reprodução.

Neste sentido, a preocupação com a transmissão dos dados também deve ser algo determinante nas mídias sociais. Um fator importante neste aspecto foi a origem da LGPD, que surgiu após a grande repercussão da divulgação de dados pessoais pela rede social Facebook. Agora, com o advento desta lei, isso se tornou inadmissível, como estabelece nos seus artigos 46, 47, 48, nos seus incisos e parágrafos, que descrevem sobre as medidas de segurança, técnicas e administrativas, que dever ser utilizadas para a proteção dos dados pessoais.

Dessa forma, pode-se depreender, a respeito da segurança no sigilo das informações das pessoas no âmbito virtual, que os responsáveis pelas mídias socias devem adotar medidas de segurança com o intuito de fornecer proteção aos dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de alteração ou utilização. Instituições públicas, financeiras, educacionais ou de telecomunicações, também possuem responsabilidade no tratamento e utilização dos dados.

Assim, a Lei Geral de Proteção de Dados adentrou no nosso ordenamento jurídico trazendo muitas novidades a respeito da proteção de dados de terceiros, transformando drasticamente a maneira com que empresas e órgãos públicos tratam a privacidade e segurança de seus usuários, que terão o exercício pleno da autodeterminação informativa em relação às suas informações.

3 ASPECTOS GERAIS DOS CRIMES DIGITAIS E AS LEGISLAÇÕES ESPECÍFICAS

Pode se considerar como crime virtual todo aquele tido dentro da seara digital. Qualquer delito ocorrido dentro da internet, ou através dela, pode ser enquadrado como um crime cibernético. Esses crimes começaram a surgir após um expressivo crescimento no número de usuários na internet, e inserido nesse número, há diversos criminosos que se aproveitaram maliciosamente desse novo invento. Deve-se levar em consideração que grande fração desse número de usuários eram pessoas leigas ou com pouca informação sobre internet, o que aumentava drasticamente a chance de se tornar vítima.

Através de invasões ou de crimes praticadas por meio de e-mails e redes sociais, era muito corriqueiro o emprego de fraude ou enganação com o intuito de "fisgar" o usuário e roubar seus dados. Esses dados se originavam de redes sociais, rede bancária, direitos autorais ou qualquer outro meio que pudesse trazer alguma vantagem ou satisfação ao criminoso.

Tanto é verdade, que os crimes mais cometidos no âmbito na internet, mais especificamente nas redes sociais e nos e-mails, são roubos de dados privados e crime contra a honra – isto envolve calúnia, injúria e difamação, ameaça, racismo, importunação sexual, homofobia e outros. Para corroborar com a ideia, Crespo ensina que:

> As denominações quanto aos crimes praticados em ambiente virtual são diversas, não há um consenso sobre a melhor denominação para delitos que se relacionam com a tecnologia, crimes de computação, delitos de informática, abuso de computador, fraude informática, em fim, os conceitos ainda não abarcam todos os crimes ligados à tecnologia, e, portanto, deve-se ficar atento, quando se conceitua determinado crime, tendo em vista que existem muitas situações complexas no ambiente virtual. (CRESPO, 2011 p. 48).

A partir do ano de 2012, foram sancionadas diversas leis que qualificam os crimes na internet de maneira específica, e que, consequentemente, alteraram o Código Penal. Uma dessas é a Lei dos Crimes Cibernéticos (12.737/2012, popularmente conhecida como "Lei Carolina Dieckmann"), que na época foi criada após crackers de Minas Gerais e São Paulo, através de um golpe por e-mail, subtraírem fotos da Carolina Dieckmann nua, fotos essas que alcançaram

mais de 8 milhões de visualizações, que para a época era um número demasiadamente expressivo. Foi tão grande a relevância do caso que a própria presidente da época resolveu intervir. O caso foi a maior contribuição para a criação do dispositivo normativo, mas também houve influência do grande volume de roubos e golpes de senhas que vinham sendo cometidos pela rede.

Cabe elucidar, acerca da problemática de inexistência de legislação específica e estudos aprofundados para diversos crimes virtuais, que delitos com um menor potencial ofensivo, como invasão de dispositivo, podem ser punidos com pena de prisão de 3 meses a 1 ano, e multa, enquanto condutas bem mais graves, como adquirir por invasão material de comunicações telefônicas privadas, segredos de indústria ou comércio, pode ter pena de apenas 6 meses até dois anos de prisão, e multa. Ou seja, ainda não há satisfatória compatibilidade e equilíbrio na tipificação dos delitos e em suas respectivas penas.

3.1 DAS PROVAS E RASTROS

Cumpre destacar a função dos provedores de conexão e provedores de aplicação. O Marco Civil da Internet tornou obrigatório aos provedores guardar informações de usuários que utilizaram determinado serviço, bem como a data e a hora em que a conexão foi realizada.

Existem também as questões relativas ao direito à privacidade, considerando que a obtenção destas informações é fundamental para a resolução de crimes, mas demandam cautela. Os registros de acesso permitem rastrear e identificar de onde surgiu determinada conduta ilícita, mas como se tratam de dados sensíveis, somente são fornecidos mediante ordem judicial. Os registros de serviço podem apontar à divulgação ou compartilhamento de conteúdo criminoso.

Cabe conceituar que o provedor de conexão é a pessoa jurídica fornecedora de serviços que possibilitam o acesso dos consumidores à Internet. Temos como principais exemplos as empresas de telefonia Tim, Claro, OI e Vivo. Já o provedor de aplicação é a pessoa natural ou

jurídica que se utiliza do acesso à internet para prestar serviços. Podemos exemplificar os provedores de conteúdo, provedores de e-mail ou de hospedagem.

As evidências de um crime tradicional mostram informações essenciais para a investigação, como testemunhas, traços, vestígios e indícios. No que tange ao crime cibernético, as evidências digitais também são vitais e são abrigadas em inúmeros dispositivos, telemáticos e informáticos, como computadores, telefones celulares, pen drives, máquinas fotográficas, provedores de Internet e registros de equipamentos de infraestrutura de rede (roteadores, firewalls, web servers, servidores de e- mail, entre outros). As provas podem ser as mais diversas possíveis: arquivos digitais, registros de servidores, *cookies*, o histórico de navegadores, fotos ou vídeos, e-mails e registros de conversas on-line.

Pela característica da evidência digital, caso a mesma não seja prontamente preservada, pode ser rapidamente danificada, perdida ou alterada, impedindo qualquer investigação ou identificação de criminosos. A coleta de vestígios digitais segue rigorosos mecanismos de preservação, além de controlar qualquer espécie de alteração. Uma característica da evidência digital é que, na maioria dos casos, ela pode ser copiada inúmeras vezes.

Nesses casos, a cópia pode ser exatamente como a original e não invalida seu uso como prova, diferentemente dos vestígios físicos. Infelizmente, o mesmo princípio se aplica para um crime cibernético: quando uma imagem ou vídeo criminoso é removido da Internet, as cópias podem ser publicadas novamente, perpetuando o sofrimento e exposição da vítima.

3.2 DO CONCEITO DE CRIME, DOS CRIMES VIRTUAIS E A SOCIEDADE

O conceito do que é crime sempre foi bastante discutido pela doutrina ou por acadêmicos. Haja vista que não há uma definição clara por parte do Código Penal, necessário se faz trilhar sobre a tríade da conceituação de crime. Dispõe Rogério Greco (2016, p. 196) que:

> Não foram poucos os doutrinadores que, durante anos, tentaram fornecer esse conceito de delito. Interessa-nos, neste estudo, refletir somente sobre aqueles mais difundidos.

> Assim, mesmo que de maneira breve, faremos a análise dos seguintes conceitos: a) formal; b) material; c) analítico.

O crime informático pode ser conceituado como o fato típico e antijurídico cometido por meio da ou contra a tecnologia da informação. Decorre, pois, do Direito Informático, que é o conjunto de princípios, normas e entendimentos jurídicos oriundos da atividade informática. Assim, é um ato típico e antijurídico, cometido através da informática em geral, ou contra um sistema, dispositivo informático ou rede de computadores. Em verdade, pode-se afirmar que, nesses crimes, a informática ou é a ofendida ou é o meio para a ofensa de direitos.

De forma breve, pode-se entender que o conceito formal é quando uma conduta colide com a lei penal vigente de um Estado, criando assim um fato típico e antijurídico. Enquanto que, materialmente, seria a conduta que afronta os bens jurídicos. Em um sentido mútuo, no aspecto analítico, esse conceito híbrido demonstra a conjuntura que se dá a tais conceitos do delito.

Em síntese, esse aspecto do crime visa dissecar elementos que compõem a infração penal para que se possa chegar à conclusão se uma conduta é típica, ilícita e culpável. Quanto aos crimes virtuais, crítico se faz definir o que são crimes virtuais satisfatoriamente. Afinal, em um mundo de constante mudança, é complexo denominar atos antigos em novos meios.

Nesta seara, nos esclarece Greco (2017):

> Ao lado dos benefícios que surgiram com a disseminação dos computadores e do acesso à Internet, surgiram crimes e criminosos especializados na linguagem informática, proliferando-se por todo o mundo. Tais crimes são chamados de crimes virtuais, digitais, informáticos, telemáticos, de alta tecnologia, crimes por computador, fraude do crime visa dissecar elementos que compõem a infração penal para que se possa chegar à conclusão se uma conduta é de ação típica, ilícita e culpável (GRECO. 2017, p 61).

Absorve-se, portanto, a falta de harmonia entre as nomenclaturas para especificar delitos ocorridos no âmbito virtual, como ensina Maria Eugênia Mendes e Natália Borges Vieira (2012 p. 55):

> No cenário dos avanços tecnológicos na área da informática, surgiram os denominados crimes cibernéticos. Porém, não existe uma nomenclatura uniformizada para os crimes dessa natureza, por isso esses crimes são denominados também de crimes de informática, crimes tecnológicos, crimes virtuais, crimes informáticos, delitos computacionais, crimes digitais, crimes virtuais, crimes cometidos por meio eletrônico, entre outros.

Ainda que exista divergência sobre uma melhor nomenclatura para esses crimes, todas remetem a uma ideia de conduta criminosa. Contudo, se não ocorre padrão para nomenclaturas, os motivos que ocasionam crimes podem ser identificados através de pesquisas e estudos de comportamento forenses, através de análise criminal, na qual se possa criar um padrão sobre a conceituação da denominação de crime virtual.

As classificações expostas são usadas como fim didático, apenas para entender e classificar certos crimes. Porém, devido a rápida evolução e alta complexibilidade da sociedade e da internet, fica praticamente impossível acompanhar e denominar corretamente as modalidades.

3.3 SUJEITOS DOS CRIMES CIBERNÉTICOS

3.3.1 Do sujeito ativo

Preliminarmente, se faz necessária a definição correta do termo hacker, este que é comumente utilizado de forma errônea pela mídia, visto que sempre utilizado negativamente. O termo significa fuçador, bem como foi popularizado por volta da década de 1960, e diz respeito ao indivíduo detentor de conhecimentos avançados de informática, de forma a possibilitar resolver problemas em computadores ou se utilizar destes para auxiliar no aumento da segurança de sistemas de dados, reconhecendo suas vulnerabilidades.

Conforme Bach (2001), o termo hacker, por sua vez, serve para designar um programador com amplo conhecimento sobre sistemas, mas sem a intenção de causar danos. Inclusive, a habilidade para lidar com sistemas e programações, muitas vezes, é aplicada pela

própria polícia em investigações ou até mesmo no desenvolvimento de softwares com o intuito de limar brechas de segurança, criar novas funcionalidades ou adaptar as antigas.

Por outro lado, temos os chamados crackers, que são agentes maliciosos que buscam invadir e roubar os dados, comprometer a segurança ou o sistema como um todo. Esses criminosos possuem conhecimentos tão vastos quanto os hackers, porém os utilizam para cometer delitos, criar ou se aproveitar de vulnerabilidades, geralmente por meio de falhas de segurança ou por meio da inexperiência e ignorância de usuários comuns.

Existem subdivisões que definem outras habilidades dos crackers, sendo as mais conhecidas as seguintes:

- Carder: especialista em roubar informações bancárias como números de cartões de crédito, cartões de conta corrente ou poupança, ou contas em sites de movimentações bancárias, para compras on-line, saques em caixas eletrônicos, transferência para contas de laranjas entre outros atos ilícitos. Assim, são consideradas pessoas que atuam em grupo ou sozinhas na Internet, cujo objetivo é conseguir dados e senhas de cartões de créditos para realizar fraudes via online. São estelionatários que analisam a vulnerabilidade de usuários que fazem compras via internet extraindo os dados da vítima e realizando compras em outros sites que são entregues em endereços de terceiros, chamados de drops.
- Defacer: especialista em pichar sites normalmente deixando mensagens de protesto contra o próprio site.
- Spammer: dissemina e-mails com correntes e vírus que podem danificar e roubar informações dos usuários, como senhas bancárias.
- Phisher: especializado em aplicar golpes diversos. Eles são profundos conhecedores das falhas de um sistema.
- Phreaker: especialista que utiliza técnicas para burlar os sistemas de segurança das companhias telefônicas, normalmente para fazer ligações de graça ou conseguir créditos.

Cabe ressaltar que a identificação desses agentes somente é possível através do endereço de IP (*Internet Protocol*), que se trata de um número que o computador -ou roteador- recebe

quando se conecta à Internet. É através desse "endereço" que o computador é identificado e pode enviar e receber dados, como se fosse uma identidade virtual. Essa identificação, por vezes, é problemática, pois os provedores não guardam tais informações por muito tempo, bem como ainda dependem de autorização judicial para divulgá-las ou utilizá-las, além de ser possível camuflá-las ou alterá-las com facilidade com o devido conhecimento técnico.

Tudo que se faz na internet deixa rastros, e é sobre essa premissa que os usuários avançados trabalham, seja para cometer crimes, encontrar os criminosos ou evitar serem encontrados por outros usuários. Independente da identificação, o sujeito ativo dos crimes é sempre quem, fazendo o uso de sua inteligência, acessa outros dispositivos ou se aproveita de vulnerabilidades com intuito de cometer delitos, ou mesmo aquele que, mesmo sem um conhecimento tão avançado, faz uso da internet com fim malicioso.

3.3.2 Do sujeito passivo

O sujeito passivo é uma figura mais fácil de descrever, podendo ser qualquer indivíduo que tenha um bem jurídico lesado ou ameaçado de lesão por ações através do computador ou qualquer outro dispositivo com acesso à rede. Pode ser tanto a Pessoa Física quanto Pessoa Jurídica.

Pode-se afirmar que, por sujeito ativo, temos aquele que efetua a conduta criminosa, enquanto que o sujeito passivo é o que sofre o dano dessa conduta. Discorre Rocha (2013, p. 55, online) que:

> O crime é um fato que viola a norma jurídico-penal, assim o sujeito ativo do delito é a pessoa humana que comete o ato ilícito pena. Não raro, os crimes são cometidos por mais de um sujeito ativo, o que caracteriza o concurso de pessoas (art.29). Por sujeito passivo deve-se entender o titular do interesse cuja a sua ofensa constitui a essência do delito. O sujeito passivo pode ser um indivíduo incapaz, mas nunca coisas ou um cadáver. Também pode ser um sujeito passivo do crime, como pessoa jurídica, sendo o exemplo eloquente dessa situação o Estado, no caso de crimes que atinjam diretamente a Administração pública ou a Administração da Justiça.

É de clareza solar a identificação entre o sujeito passivo e ativo de um crime em ambiente cibernético, visto que qualquer pessoa pode ser vítima de um delito virtual, bastando ter acesso à internet e um dispositivo capaz de navegar na rede. (ROCHA, 2013)

O grande obstáculo hoje é a identificação do sujeito ativo. É bastante comum que o acesso seja realizado na rede pública, no qual não há a necessidade de informar dados pessoais para ser utilizada, ou por programas que mascaram o endereço do computador, o já citado IP. Como mostra Pedro Pisa (2016 p. 48), "O IP (*Internet Protocol*) é o principal protocolo de comunicação da Internet. Ele é o responsável por endereçar e encaminhar os pacotes que trafegam pela rede mundial de computadores".

Assim, para se descobrir o real sujeito ativo do crime virtual, é necessário localizar o local ou dispositivo de acesso usado pelo agente criminoso através do IP. Discorrem sobre o tema Emerson Wendt e Higor Vinicius Nogueira Jorge (2013 p. 13):

> (...) quando ocorre a conexão com um computador ou dispositivo similar à internet (como celular, tablet, etc.) o endereço de I.P (Internet Protocol) é atribuído, exclusivamente, para aquele internauta. Da mesma forma que dois corpos não ocupam o mesmo lugar no espaço, não existem dois usuários com o mesmo IP durante a navegação da internet, independente do endereço de IP ser estático ou dinâmico.

É possível observar que, no que tange à identificação do sujeito passivo, basta analisar qual o bem tutelado pela norma e a quem pertence, enquanto para identificar o agente causador da lesão ao sujeito passivo, se faz necessário muito trabalho e grandes despesas de recursos, tornando inviável, por muitas vezes, alcançar o criminoso responsável.

3.4 DO LOCAL E O TEMPO

Grande obstáculo enfrentado pelo ordenamento jurídico é a especificação do foro competente para o julgamento dos delitos cibernético, afinal, há possibilidade de que uma pessoa esteja em qualquer país do mundo e cometa um crime no Brasil através da Internet, aumentando significativamente a dificuldade de identificar o momento e o local do fato criminoso. Sobre o tema, afirma Gabriel Cesar Zaccaria de Inellas (2004 p. 79) que "Como a

rede da internet é mundial e sem fronteiras e sem donos, torna-se quase impossível para qualquer país, aplicar e executar leis, para regular o denominado ciberespaço".

O Direito Penal utiliza-se do princípio da ubiquidade para lidar com a territorialidade do ato virtual criminoso, este entendendo que o lugar do crime é onde o delito foi praticado e, ao mesmo tempo, onde se consumou.

Acerca do tema, explicam Barreto e Brasil (2016, p. 26) que:

> No caso dos delitos cibernéticos, mais apropriada é a adoção da Teoria da Ubiquidade, por ser mais completa, pois, com a volatilidade das evidências de crimes digitais, aliada ao fluxo intenso de informações, nem sempre será possível definir com clareza onde ocorreu a ação e onde houve o resultado. Em muitas ocasiões nem o criminoso nem a vítima está no local onde se consumou a ação delituosa, nem foi neste que houve o abalo social.

A teoria é a mais aceita pela doutrina e pela legislação, assim como afirma que pouco importa o local da prática ou da consumação, ambos os locais serão competentes para lidar com a situação. Portanto, quando um delito virtual é cometido fora do Brasil, mas se consuma neste, deve ser considerado como um crime praticado em território nacional. (JESUS, 2001)

Por outro lado, o artigo 7º do Código Penal expõe os princípios da teoria da extraterritorialidade, aplicável aos crimes cometidos fora do território, mas com repercussão neste:

> 1. Princípio da Proteção (art. 7º, inciso I, §3º), segundo o qual prevalece a lei referente à nacionalidade do bem jurídico lesado, é também conhecido como Princípio da defesa real;
> 2. Princípio da Justiça Universal (art. 7º, inciso II, alínea a), aplica-se a lei brasileira aos crimes que por tratado ou convenção internacional o Brasil se obrigou a punir;
> 3. Princípio da Nacionalidade Ativa (art. 7º, inciso II, alínea b), aplica-se a lei nacional aos brasileiros, onde quer que estes se encontrem;
> 4. Princípio da Representação (art.7 º, inciso II, alínea c), que torna possível a aplicação da lei brasileira aos crimes cometidos no estrangeiro em aeronaves ou embarcações privadas ou mercantes que se localizem em território alienígena e aí não sejam julgados.

Por fim, no que concerne à definição do tempo do crime, o nosso Código Penal e a doutrina melhor aceitam a teoria da atividade, onde a prática do crime será considerada a partir

do momento da ação ou omissão, independentemente de qual for o momento do resultado. (BRASIL, 1940)

Pode-se observar que o Código Penal lida com os delitos cibernéticos de forma principialista, por isso se faz necessário uma legislação mais detalhada em conjunto com um tratamento internacional que especifique quem possuirá competências para julgar o crime virtual, a fim de lidar com as situações delituosas mais comuns no âmbito do ciberespaço. Somente dessa forma, poderá ser utilizado o Direito Penal para alcançar os cibercriminosos que se escondem na distância.

3.5 LEGISLATIVA BRASILEIRA

Por ser vasto o ciberespaço, requer uma melhor análise legislativa no que diz respeito aos agentes delituosos, haja vista que a falta de tipificação de condutas prejudica a aplicação da pena. A seguir, serão demonstrados alguns dispositivos normativos que tratam do assunto.

A Lei nº 12.737/2012, em seu artigo primeiro, traz expresso: "Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências" (BRASIL, 2012). A inovação legislativa tipificou alguns crimes virtuais no Código Penal.

Foram inseridos os seguintes tipos penais derivados da Lei em comento: Invasão de dispositivo informático (Art. 154-A, CP); Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública (Art. 266, CP); Falsificação de documento particular, Falsificação de cartão (Art. 298, CP).

Damásio de Jesus afirma que:

> Apelidada de "Lei Carolina Dieckmann", a Lei n. 12.737/2012, que tipifica os crimes cibernéticos, adveio do projeto de Lei n. 2.793/20115, sendo agilizado no início de 2013 pelo "casuísmo em que fotos íntimas da atriz teriam sido supostamente copiadas de seu computador e divulgadas na internet". Na verdade, a legislação veio atender a uma demanda antiga do setor financeiro, duramente impactado com os golpes e fraudes eletrônicas, ainda que considerada uma lei absolutamente "circunscrita", em

> comparação aos projetos sobre crimes cibernéticos que tramitavam no congresso nacional. Entendeu-se em aprovar uma lei menor, com pontos menos polêmicos, a não ter nada regulamentando crimes cibernéticos, eis que, diz o ditado, a lei é como remédio, deve ser ministrado em doses, pois se ministrarmos tudo de uma vez, podemos matar o paciente (JESUS, 2014, p.85).

Importante salientar que esta Lei, como citado acima, veio devido a uma demanda de setores prejudicados por esses tipos de condutas, porém, o fato que levou o assunto a uma repercussão nacional, foi quando a atriz que dá nome à norma teve suas fotos íntimas vazadas na internet, ou seja, houve uma grande dificuldade para os operadores do Direito no que tange ao enquadramento da conduta que carecia de tipificação legislativa.

Já a Lei nº 14.155, uma das mais recentes novidades legislativas, promulgada no ano de 2021, vai ao encontro dos temas referentes aos crimes virtuais ou praticados em ambientes virtuais, alterando o Código Penal e o Código de Processo Penal. Importante mencioná-la, tendo em vista os dispositivos penais que careciam de tipificação mais específica e rigorosa, estando entre as alterações trazidas por ela a inclusão do crime de perseguição, também conhecido como *stalking* (Art. 147-A, CP). Também foram alterados os crimes de invasão de dispositivos informáticos (Art. 154-A, CP), furto mediante fraude eletrônica (Art. 155, § 4º-B, CP), estelionato mediante fraude eletrônica (Art. 171, § 2º-A, CP), entre outros.

Segue o embasamento do senador Izalci Lucas (2020), à época, para apresentação do referido Projeto de Lei:

> O Jornal Folha de São Paulo de 26/08/2020 noticia que a pandemia fez aumentar drasticamente o número de fraudes cometidas de forma eletrônica, gerando perdas de aproximadamente R$ 1 bilhão. Segundo a mesma fonte, a alta foi de 70% e os montantes envolvidos já se apresentam como empecilho à redução de juros ao consumidor, vez que se elevaram os riscos envolvidos. Esse tipo de crime tem atingindo, inclusive, os beneficiários do auxílio emergencial. Estima-se que 600 mil fraudes foram praticadas somente no pagamento do benefício. São inúmeros os canais de imprensa que vem noticiando a explosão de ocorrências em que criminosos estão lucrando durante a pandemia. Observa-se que tem havido um aumento crescente de crimes dessa natureza nos últimos anos, mas que o número disparou durante a pandemia. A situação agrava-se ainda mais quando os servidores de rede utilizados para o crime estão situados fora do país. O Banco Central emitiu alerta sobre fraudes durante a pandemia, quando os golpes via WhatsApp ultrapassaram 11 milhões de casos. Bandidos usam inclusive aplicativos de informação sobre o Coronavirus para enganar os cidadãos de bem. Nosso país alcançou o terceiro lugar no ranking mundial em registros de fraudes eletrônicas. Os criminosos, em função da branda legislação brasileira, estão escolhendo o Brasil como terreno fértil para seguirem impunes. O

> Jornal O Globo de 14 de julho informa inclusive que os cibercriminosos brasileiros estão expandindo suas atividades aplicando fraudes nos Estados Unidos, Europa e China. Líderes em segurança contra fraudes lamentam todo o esforço para combater esse tipo de crime enquanto a legislação considerar essa prática como um crime menor, cujas penas são muitas vezes substituídas por penas "alternativas". O volume de fraudes já começa a afetar a economia do país, gerando perda do poder aquisitivo e também perdas emocionais por parte das vítimas. Diante do exposto, é medida urgente que aprovemos meios mais rigorosos para punir esse tipo de crime que assola o país.

O crime de invasão de dispositivo, bem como de alteração ou destruição de dados e instalação de vírus (malware) para obtenção de vantagem ilícita, passaram a ser punidos com reclusão de 1 a 4 anos, e multa, tendo como causa de aumento, de um terço a dois terços, se da invasão se resulte em prejuízo financeiro ou econômico. A pena anterior previa somente detenção de 3 meses a um ano. (BRASIL, 2021)

Isso demonstra que a legislação brasileira está evoluindo e buscando se adequar em relação aos crimes virtuais, contribuindo ainda mais para o combate à impunidade das condutas que carecem de previsão legislativa. Contudo, por se tratar de uma Lei recente (levando em consideração a data de elaboração deste trabalho), ainda não se tem muitos comentários e estudos a respeito dela.

Por último, ainda se faz necessário destacar a urgência na criação de um novo código que possa auxiliar a comunidade cibernética, na disseminação de canais de denúncias juntamente a banco de dados de delegacias especializadas, adequadas a esses atendimentos, aumento de atividade pericial informática e a criação de núcleos técnicos para o desenvolvimento de profissionais da área. Esses são meios de minar a atividade de agentes delituosos e trazer mais segurança aos usuários, bem como representa o que já vem sendo implementado lentamente em vários estados.

3.5.1 Novos tipos de crimes cibernéticos

Com a evolução da internet, e por consequência, dos crimes cibernéticos, não somente se modificou a forma com que os bens jurídicos já tutelados no ordenamento jurídico são

atingidos, mas também houve inovações no que tange à violação de bens jurídicos até então não alcançados, ou até mesmo surgiram formas completamente novas de atingi-los. Mostraremos a seguir, alguns delitos bastante específicos e novos, alguns ainda carecendo de legislação própria e debates aprofundados.

O primeiro novo tipo de crime virtual que vale expor é o *Revenge Porn.* O referido termo é uma expressão que foi criada nos Estados Unidos, possuindo o conceito de pornografia de vingança ou pornografia de revanche. É usado para se referir à divulgação de fotos, vídeos, áudios, montagens, ou qualquer outro material sexualmente gráfico, íntimo e privado, sem a devida autorização, com a finalidade de exposição da vítima e causar danos.

Sobre o conceito do termo, afirma Fátima Burégio que:

> O termo consiste em divulgar em sites e redes sociais fotos e vídeos com cenas de intimidade, nudez, sexo à dois ou grupal, sensualidade, orgias ou coisas similares, que, por assim circularem, findam por, inevitavelmente, colocar a pessoa escolhida a sentir-se em situação vexatória e constrangedora diante da sociedade, vez que tais imagens foram utilizadas com um único propósito, e este era promover de forma sagaz e maliciosa a quão terrível e temível vingança (BURÉGIO, 2015, online).

As vítimas dessa divulgação não-consensual, expostas na internet para o livre acesso de qualquer pessoa interessada, passam a sentirem-se humilhadas, intimadas, perseguidas e assediadas, em um ciclo que é conhecido pela teoria feminista como *slut-shaming.*

Considerando a frequência que os casos ocorriam, se demonstrou necessário adotar uma legislação que trouxesse a pena adequada para as condutas, a fim de coibir sua prática, eis que a maioria dos réus não eram condenados ou não ficavam presos.

Ademais, para que fossem solucionadas as divergências e considerando o crescente número de casos, a conduta passou a ser considerada crime, mediante a implementação da Lei nº 13.718/18, inserindo novos delitos no texto do Código Penal. Surgiu, por conseguinte, a figura do crime de divulgação de cena de estupro ou de cena de sexo ou pornografia, conforme abaixo relacionado, artigo 218-C, *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:
> Pena - reclusão, de 1 (um) a 5 (cinco) anos, se o fato não constitui crime mais grave.
> §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.
> §2º Não há crime quando o agente pratica as condutas descritas no caput deste artigo em publicação de natureza jornalística, científica, cultural ou acadêmica com a adoção de recurso que impossibilite a identificação da vítima, ressalvada sua prévia autorização, caso seja maior de 18 (dezoito) anos.

No Livro "Exposição Pornográfica Não Consentida na Internet", os autores Spencer Sydow e Ana Laura Castro contribuíram com a seguinte divisão detalhada do *caput* do artigo supracitado:

> (a) a divulgação do registro do crime de estupro, possibilitando que o agente seja penalizado por incidir em ambos os tipos, (b) a apologia ou indução à prática do crime de estupro, atividade que diz respeito apenas ao uso de fotografia, vídeo ou outro registro audiovisual visando estimular o referido crime, e busca atingir especialmente a disseminação de sítios voltados à propagação de discursos de ódio que fomentam crimes sexuais, e (c) registros de cenas de sexo, nudez ou pornografia sem o consentimento da vítima (CASTRO, SYDOW, 2019, p. 134).

Para os autores, o legislador quis que fosse preservada a dignidade, intimidade e privacidade, sendo afastada somente a proteção específica da honra, já que a mesma possui caráter subjetivo de prejuízo à vítima. Destacam, também, que a consumação pode ser tanto instantânea quanto permanente, pois o agente é o que possui o poder de parar a conduta lesiva, vindo assim a gerar a possibilidade de tentativa.

Outro tipo de crime virtual moderno é a *sextorsão*, a qual é oriunda da junção dos vocábulos sexo e extorsão. É um neologismo originado nos Estados Unidos, no ano de 2010, quando foi utilizado oficialmente pelo FBI, em um caso onde um hacker chantageou mulheres, vindo a ameaçar expor dados e informações íntimas privadas, caso não fossem atendidas as exigências de enviar novas fotos nuas. A globalização e a difusão da internet no Brasil potencializaram a capacidade de disseminação das informações, e por consequência, das inovações delitivas, vindo a tornar assim o termo mais conhecido.

Trata-se de uma situação onde a posição de poder do criminoso é utilizada como um instrumento para obter a vantagem de cunho libidinoso, se aproveitando do medo e vergonha da vítima, sendo portanto, uma forma de chantagem *online* que se dá pelo constrangimento de uma pessoa à prática sexual ou pornográfica registrada em foto ou vídeo para envio, em troca de ser mantido o sigilo, mas não possuindo qualquer garantia de que as ameaças não se concretizarão mesmo após a vítima ceder às chantagens.

O Promotor de Justiça e professor de Direito Penal e Processo Penal, Rogério Sanches Cunha, afirma que:

> A prática que passou a ser conhecida como *sextorsão* refere-se a uma forma de exploração sexual na qual a vítima é chantageada através da ameaça de publicação de imagens e vídeos de si mesma, dotadas de cunho sexual, previamente compartilhadas mediante *sexting* ou subtraídas de seus arquivos pessoais digitais, objetivando a obtenção de alguma vantagem. Nessas situações é comum que a vítima seja constrangida a enviar mais mídias de conteúdo erótico ao agressor, constantemente sob a ameaça de divulgação tanto do conteúdo original quanto deste último obtido sob chantagem (CUNHA, 2019*, online).*

Por conseguinte, observa-se que no Brasil, não existe uma adequação típica específica para o crime, gerando insegurança jurídica e a sensação de impunidade, além de esbarrar no princípio da proibição da analogia e da estrita legalidade adotados pelo ordenamento jurídico brasileiro. O delito acaba por ser muitas vezes interpretado como estupro virtual, em casos graves, ou outros crimes mais brandos, de forma a ser aplicado substitutivamente algum dispositivo penal que pareça cabível, mesmo que inadequada ou insatisfatoriamente, ao caso concreto, a fim de suprir a lacuna legislativa existente.

Outro tipo de delito cibernético é o estupro virtual, sendo considerado um estupro que é caracterizado pela não utilização da força física para dominar a vítima, já que no âmbito da internet somente é possível empregar a violência por meio do domínio psicológico, se resumindo a ameaças, chantagens e constrangimentos.

Quanto a possibilidade da configuração do crime de estupro sem a necessidade de contato físico, por meio eletrônico, afirma Fernando Capez:

> A hipótese em comento não se confunde com aquela em que a vítima é obrigada a práticas atos libidinosos em si própria, como a masturbação para que o agente a contemple lascivamente. Embora nesses casos não haja contato físico entre ela e o agente, a vítima foi constrangida a praticar ato libidinoso em si mesma. Surge aí a chamada autoria mediata ou indireta, pois o ofendido, mediante coação moral irresistível, é obrigado a realizar o ato executório como longa manus do agente (CAPEZ, 2017, p. 23).

No ano de 2017, no Estado do Piauí, existiu o primeiro caso conhecido de estupro virtual no Brasil, vindo a tornar-se de extrema relevância para o ordenamento jurídico. O tema ainda é muito debatido por não haver uma posição pacificada sobre o assunto, porém o Supremo Tribunal Federal interpretou que o contato físico é dispensável para que seja configurado o tipo penal presente no artigo 213 do Código Penal, confirmando o entendimento em decisão proferida no ano de 2017 ao julgar o Recurso Extraordinário com Agravo nº 1066864 RS.

Na decisão, afirma o Ministro Dias Toffoli:

> "(...) a maior parte da doutrina penalista pátria orienta no sentido de que a contemplação lasciva configura o ato libidinoso constitutivo dos tipos dos Arts. 213 e 217-A do Código Penal - CP, sendo irrelevante, para a consumação dos delitos, que haja contato físico entre ofensor e ofendido. (...) Com efeito, a dignidade sexual não se ofende somente com lesões de natureza física. A maior ou menor gravidade do ato libidinoso praticado, em decorrência a adição de lesões físicas ao transtorno psíquico que a conduta supostamente praticada enseja na vítima, constitui matéria afeta à dosimetria da pena, na hipótese de eventual procedência da ação penal (...)." (DIAS, 2018, ONLINE).

No ano de 2019, em São Paulo, um rapaz de 25 anos, mantinha contato com uma mulher via rede social *WhatsApp* e, quando obteve sua confiança, convenceu a vítima a lhe enviar fotos íntimas. Posteriormente, ao receber ameaças, foi obrigada a enviar foto pornográfica de sua filha. Nesse caso, é possível enquadrar o fato ao tipo penal de estupro, partindo do advento da Lei nº 12.015/2009, que trouxe atualizações ao capítulo dos crimes contra a dignidade sexual.

Cabe também destacar a prática do *sexting* e a exposição íntima não autorizada. O termo é utilizado para se referir à exposição do corpo nu ou seminu em virtude de desejo próprio ou de terceiros, através de tecnologias digitais, sendo usado para expressar a sexualidade. No entanto, o problema aparece quando as referidas imagens são expostas sem ter a permissão e o

consentimento da vítima, vindo a gerar um constrangimento público ou danos, muitas vezes irreparáveis.

Sobre o assunto, afirma Suzana da Conceição Barros:

> O sexting consiste no envio, compartilhamento e postagem de mensagens eróticas, fotos de corpos desnudos e de vídeos que mostram relações sexuais, ou seja, de materiais que apresentam conteúdos sexuais, sensuais e eróticos, por meio de tecnologias digitais (smartphones, tablets, computadores, e sites de redes sociais, como Facebook e Twitter etc.), para namorados/as, ficantes, paqueras, amigos/as, ou para uma multidão de conhecidos/as e desconhecidos/as, quando postados na internet, por exemplo. Crianças, adolescentes, adultos, isto é, sujeitos de diferentes faixas etárias, vêm aderindo a essa prática (BARROS, 2019, ONLINE).

Assim, entende-se que *sexting* é uma conduta que coloca em risco os direitos da personalidade, intimidade, honra e da boa fama, já que pode provocar consequências à imagem, por tempo indeterminado. Assim, é imperioso que sejam criados tipo penais específico para a conduta, assim como as demais, com penas proporcionais ao sofrimento causado às vítimas.

3.5.2 Delegacias especializadas em crimes informáticos

A Lei nº 12.735/2012, popularmente conhecida como "AI-5 digital", trouxe a possibilidade de criação de delegacias especializadas em repressão de crimes cibernéticos, ao dispor que "os órgãos da polícia judiciária estruturem setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado". (BRASIL, 2012)

Essas delegacias possuem a incumbência de reprimir a prática dos crimes cibernéticos, dispondo de equipamentos e conhecimentos indispensáveis para proceder às investigações de maneira mais eficiente, bem como a função de atender às vítimas desses delitos, dando o suporte necessários à defesa e proteção dos bens jurídicos lesados.

Na cidade de São Paulo, por exemplo, em 15 de outubro de 2020, foi criada pelo governador João Dória a Divisão de Crimes Cibernéticos (DCCIBER), sendo o órgão subordinado ao Departamento Estadual de Investigações Criminais (DEIC). Anteriormente, só havia uma delegacia em todo estado de São Paulo que fazia investigação de crimes cibernéticos. (G1, 2020)

O cibercrime é considerado como toda atividade delitiva onde um computador ou uma rede de computadores é utilizada como uma ferramenta, e essas práticas podem ser denunciadas aos órgãos de polícia judiciária da mesma forma que os crimes ocorridos fora do ambiente virtual. Cabe ressaltar, entretanto, que os referidos órgãos vêm se adaptando lenta e tardiamente, eis que ainda não há treinamento e estrutura suficientes para prestar de forma eficiente tal serviço, seja pela atualidade do tema, ou pela falta de recursos destinados pelos órgãos competentes.

Dentre os crimes virtuais mais recorrentes, foi identificada uma especial crescente de ataques *Ransomwares*, sendo esse um tipo de malware que bloqueia o sistema ou os dados e exige "resgate", ou seja, uma forma de extorsão virtual. Essas ameaças, conforme previamente destacado, geralmente se instalam através de vulnerabilidades do computador da vítima ou por descuido no uso da rede, muito comumente por meio da prática do *Phishing*, onde a vítima acessa arquivo, link ou mensagem e acaba por ser invadida.

De acordo com o G1 (2021), "O Brasil é o 5º maior alvo dessa ameaça, com 9 milhões de tentativas de ataques, segundo um relatório da empresa de cibersegurança SonicWall". Há uma preocupação muito grande com a privacidade e segurança de forma geral, de toda a sociedade, considerando que as grandes empresas, que são os alvos mais recorrentes desses crimes, guardam, em seus bancos de dados, as informações pessoais, financeiras e íntimas de milhares de usuários, essas que podem ser roubas e utilizadas de forma maliciosa. A LGPD também não deixa claro se a empresa deve comunicar esses ataques aos titulares dos dados.

4 ANÁLISE JURISPRUDENCIAL DOS CRIMES VIRTUAIS

Em casos que tratam de divulgação e compartilhamentos de dados, mensagens ou imagens de terceiros de forma não autorizada, o controlador, por sua vez, deverá comunicar esses casos às autoridades públicas o mais rapidamente possível, devendo fornecer a descrição da natureza dos dados pessoais afetados, as informações sobre as pessoas envolvidas na ocorrência, a indicação das medidas técnicas e de segurança utilizada para o fornecimento de proteção dos dados, observando os segredos comercial e industrial, os riscos relacionados à ocorrência, demonstrar os motivos da demora, no caso da comunicação não ser imediata, bem como expor as medidas que foram ou que deverão ser adotadas, com o intuito de reverter ou reduzir os efeitos do prejuízo.

Aquele que divulga, controla ou se utiliza de dados de terceiros de forma indevida, mesmo que no livre exercício de sua profissão, estará violando os direitos à intimidade e vida privada, podendo ser responsabilizado nas esferas criminal e cível. Podemos exemplificar a função dos jornalistas e das emissoras de televisão, que possuem responsabilidade sobre a veracidade e uso indevido dessas informações.

É demonstrado a seguir, Recurso extraordinário com agravo, cuja decisão foi provida pelo Supremo Tribunal Federal sobre o tema:

> RECURSO EXTRAORDINÁRIO COM AGRAVO. CIVIL. DANO MORAL. DIREITO DE IMAGEM. MATÉRIA COM REPERCUSSÃO GERAL REJEITADA PELO PLENÁRIO DO STF NO ARE Nº 739.382. CONTROVÉRSIA DE ÍNDOLE INFRACONSTITUCIONAL. SOBRESTAMENTO. PENDÊNCIA DE RECURSO NO SUPERIOR TRIBUNAL DE JUSTIÇA. 1. O dano moral, quando aferido pelas instâncias ordinárias, não revela repercussão geral apta a dar seguimento ao apelo extremo, consoante decidido pelo Plenário virtual do STF, na análise do ARE nº 739.382, da Relatoria do Min. Gilmar Mendes. 2. A pendência de recurso no Superior Tribunal de Justiça não implica no sobrestamento do extraordinário, quando o apelo extremo não possuir condições de admissibilidade. Precedentes: AI 488.301-AgR, Rel. Min. Eros Grau, Primeira Turma, DJ 17/9/2004 e AI 199.995-AgR, Rel. Min. Marco Aurélio, Segunda Turma, DJ 6/2/1997. 3. In casu, o acórdão originariamente recorrido assentou: "AÇÃO DE INDENIZAÇÃO POR DANOS MORAIS Depósito do valor da condenação com fundamento no artigo 57, § 6º da Lei de Imprensa Atitude que não se mostra incompatível com a vontade de recorrer, haja vista que à época da interposição do recurso, referido diploma legal continuava em vigor, só tendo sido reconhecida sua não recepção pela Constituição Federal de 1988

> no ano de 2009, com a ADPF 130 Recurso conhecido - Publicação de notícia divulgando declarações concedidas pelos autores ao jornalista via e-mail associada à divulgação de frame de página pessoal dos autores na internet, onde estes publicaram fotos de sua intimidade Alegação de que não houve autorização para a publicação das fotografias tampouco das declarações, sendo estas últimas deturpadas. Comprovação de que o jornalista limitou-se a publicar a declaração expressamente autorizada por um dos autores via e-mail - Ausência de animus injuriandi vel diffamandi - Fotografias que foram disponibilizadas voluntariamente pelos próprios autores na internet, permitindo-se o acesso irrestrito a todos os usuários da rede. Ausência de violação à intimidade e privacidade Publicação de nota sugerindo que um dos autores possui boneco com suas características. Não comprovação da veracidade da informação, restando caracterizado o caráter ofensivo da publicação. Danos morais configurados que devem ser fixados com razoabilidade Litigância de má-fé Não configuração - Inversão dos ônus da sucumbência – Recurso parcialmente provido. Órgão julgador: Primeira Turma Relator(a): Min. LUIZ FUX Julgamento: 29/10/2013 Publicação: 19/11/2013. (Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stf/24655778/inteiro-teor-112141306. Acesso em: 20 jul. 2022).

Segue outra jurisprudência que aponta julgado, em sede de apelação, do Tribunal de Justiça de São Paulo sobre o mesmo tema:

> Apelação cível. Ação de obrigação de fazer contra Facebook; Twitter; Google; Rede Record TV e Universo Online S/A UOL. Pedido para remoção de conteúdo envolvendo vida privada de pessoa pública (jornalista e apresentadora famosa). Divulgação de notícias envolvendo detalhes de processo judicial entre autora e antigo namorado, inclusive aspectos financeiros, agressões físicas e infidelidade conjugal. Exposição pública da intimidade pessoal. Repercussão dos fatos sobre imagem pública da autora. Sentença de procedência, com determinação de remoção de publicações sobre o mesmo fato (futuramente). Decisão de extinção do feito com relação a corré Google. Apelo das corrés Facebook; Twitter e Universo Online. Ilegitimidade passiva. Rejeição. Conteúdo armazenado pelas corrés. Legitimidade evidenciada. Remoção de conteúdo. Marco Civil da Internet. Postagem em rede mundial de computadores envolvendo vida privada de pessoa pública. Remoção determinada em razão de violação intimidade e vida privada. Determinação para evitar publicações futuras de conteúdo similar. Questão resolvida pela aplicação da regra do art. 19 e 20 da MCI. Decisão irretocável. Motivação do decisório adotado como julgamento em segundo grau. Inteligência do art. 252 do RITJ. Sucumbência. Condenação da parte vencida em custas e despesas processuais. Aplicação do princípio da causalidade. Manutenção da condenação. Honorários recursais. Aplicação da regra do artigo 85, §11, CPC/2015. Verba honorária majorada para R$8.000,00 (oito mil reais). Resultado. Preliminar rejeitada. Recursos não providos Apelação Cível nº 1001965-91.2018.8.26.0704 - São Paulo - Voto nº 30468 M (Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-sp/1258146701/inteiro-teor-1258146722. Acesso em: 27 jul. 2022).

No caso em tela, as corrés Rede Record TV e Universo Online UOL, em sede de liminar, foram compelidas a providenciarem as seguintes determinações:

> "Com a detida análise do processo, percebe-se, ainda que em juízo perfunctório, que há probabilidade do direito invocado. Com efeito, aparentemente as reportagens em questão violam os direitos à intimidade e à vida privada da autora e devem prevalecer em detrimento dos direitos de liberdade de pensamento e de expressão, na hipótese em apreço. Isso porque, não há interesse público na divulgação da entrevista em questão, que trata de assuntos peculiares à vida íntima da autora e de seu ex-namorado. Ademais, em juízo de delibação, não parece que se trata de tema que a própria autora, embora se trate de figura pública, tenha exposto abertamente à mídia. Existe igualmente o fundado risco de dano de difícil reparação consistente no fato de que o conteúdo se encontra em destaque atualmente na mídia. Ante o exposto, DEFIRO a antecipação dos efeitos da tutela para determinar às requeridas REDE RECORD TV e UNIVERSO ONLINE S/A UOL que retirem, no prazo de 24 horas, todas as publicações e postagens que versem a respeito do tema descrito na petição inicial, assim como abstenham-se de realizar novas publicações sobre o mesmo assunto, sob pena de incorrerem em multa diária de R$ 10.000,00. Deixo, entretanto, de deferir o pedido liminar em face do provedor de pesquisa e das redes sociais, por entender que não há interesse de agir em relação a estas partes, uma vez que já conhecidas as fontes das informações com conteúdo aparentemente ofensivo. Neste sentido: "CIVIL E CONSUMIDOR. INTERNET. RELAÇÃO DE CONSUMO. INCIDÊNCIA DO CDC. GRATUIDADE DO SERVIÇO. INDIFERENÇA. PROVEDOR DE PESQUISA. FILTRAGEM PRÉVIA DAS BUSCAS. DESNECESSIDADE. RESTRIÇÃO DOS RESULTADOS. NÃO-CABIMENTO. CONTEÚDO PÚBLICO. DIREITO À INFORMAÇÃO. (...) 8. Preenchidos os requisitos indispensáveis à exclusão, da web, de uma determinada página virtual, sob a alegação de veicular conteúdo ilícito ou ofensivo - notadamente a identificação do URL dessa página - a vítima carecerá de interesse de agir contra o provedor de pesquisa, por absoluta falta de utilidade da jurisdição. Se a vítima PODER JUDICIÁRIO TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO Apelação Cível nº 1001965-91.2018.8.26.0704 - São Paulo - Voto nº 30468 M 4 identificou, via URL, o autor do ato ilícito, não tem motivo para demandar contra aquele que apenas facilita o acesso a esse ato que até então, se encontra publicamente disponível na rede para divulgação. 9. Recurso especial provido. (REsp 1316921/RJ, Rel. Ministra NANCY ANDRIGHI, Terceira Turma, DJU 26/06/2012)." Intimem-se os Representantes legais da rés a respeito desta decisão. Servirá cópia da presente decisão como ofício ao Representante Legal da ré. Por não vislumbrar na espécie, diante da natureza da controvérsia posta em debate, a possibilidade de composição consensual, deixo de designar a audiência a que alude o disposto no artigo 334 do Código de Processo Civil. Citemse os réus para integrarem a relação jurídico-processual (CPC, artigo 238) e oferecerem contestação, por petição, no prazo de 15 (quinze) dias úteis (CPC, artigos 219 e 335), sob pena de revelia e presunção de veracidade das alegações de fato aduzidas pela autora (CPC, artigo 344), cujo termo inicial será a data prevista no artigo 231 do CPC, de acordo com o modo como foi feita a citação (CPC, artigo 335, III). Intime-se." Em sequência, manifestações das corrés, no seguinte sentido: (i) Facebook Serviços Online do Brasil Ltda apresentou contestação (fls. 128/153). Inicialmente, alega que sua plataforma identificou único material, já removido. Alega ilegitimidade de parte. Acrescenta que não pode ser compelida monitorar conteúdo preventivo e que

> não pode ser condenada à ordem judicial genérica. Visa ainda, afastar condenação em sucumbência. (ii) Twitter Brasil Rede de Informação Ltda apresentou contestação (fls. 199/217). Alega ilegitimidade de parte, bem como, aponta argumentos à afastar imposição para remoção de material genérico. (iii) Google apresentou pedido de habilitação nos autos, deferida (fl. 301). Contestação (fls. 303/329) alegando ilegitimidade de parte e impossibilidade ser compelida remoção de conteúdo genérico, inclusive, sobre indexação (Google Search). Aponta remoção de conteúdo (fls. 307/308). Argumenta que não pode evitar postagem de futuro material. (iv) Rádio e Televisão Record S/A apontando remoção do conteúdo: https://www.facebook.com/BalancoGeral/videos/1613 445388770373/." (fl. 43). Também apresentou aclaratórios afirmando que não pode ser compelida à remoção de conteúdo futuro ou sem identificação específica. Apresentou contestação (fls. 66/72). Diz que o material de viés jornalístico sem cunho ofensivo. (v) Universo Online requerendo dilação de prazo para cumprimento da decisão liminar, vez que o feito tramita em segredo de justiça, sendo deferida sua habilitação (fl. 44). Justificou realizar mera hospedagem de conteúdo de sites, não sendo responsável sobre teor independente, feito por terceiros. Alega ilegitimidade de parte. Apresentou contestação (fls. 80/102) reiterando argumentos. Diz que não pode ser compelida à cumprimento de ordem genérica, além de apontar que a decisão veda liberdade de expressão e não PODER JUDICIÁRIO TRIBUNAL DE JUSTIÇA DO ESTADO DE SÃO PAULO Apelação Cível nº 1001965-91.2018.8.26.0704 - São Paulo - Voto nº 30468 M 5 há conteúdo lesivo (Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-sp/1258146701/inteiro-teor-1258146722. Acesso em: 20 out. 2022).

A tais razões de decidir, acrescente-se que o feito versa sobre remoção de conteúdo disponibilizado na internet envolvendo intimidade de vida privada de pessoa famosa e detalhes de processo judicial entre autora e antigo namorado, com insinuações públicas de auxílio financeiro do homem, agressões físicas e infidelidade conjugal. No caso, houve exposição pública de intimidade pessoal, sem interesse à sociedade, conforme Lei nº 12.965/2014 (Marco Civil da Internet), artigo 19, *in verbis*:

> Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário. § 1º A ordem judicial de que trata o caput deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material. (MCI)

É possível depreender que este preceito legal se destina aos tratamentos de dados pessoais, inclusive na esfera digital, por pessoa natural ou pessoa jurídica, objetivando a proteção dos direitos fundamentais, sendo estes: da liberdade, dignidade da pessoa humana,

privacidade e do livre desenvolvimento da personalidade natural, estando esses princípios fundamentados na Constituição Federal de 1988.

Através dessas decisões dos Tribunais, pode-se constatar que se está criando o entendimento de que às vítimas, cabe o direito indenizatório sobre os crimes cibernéticos sofridos, no que concerne às suas informações digitais.

Conforme já analisado, o maior desafio legislativo no Brasil é quanto à inexistência de legislação específica para diversos crimes cometidos no âmbito da internet, e abaixo será demonstrado como alguns tribunais vêm atuando no que diz respeito aos crimes virtuais em geral, diante do cenário de carência legislativa expressiva.

Segue jurisprudência relativa ao crime de furto qualificado cometido por intermédio da rede mundial de computadores:

> PENAL. PROCESSUAL PENAL. HABEAS CORPUS. FURTO QUALIFICADO ATRAVÉS DA REDE MUNDIAL DE COMPUTADORES. APELAÇÃO EM LIBERDADE. IMPOSSIBILIDADE. PACIENTE PRESO EM OUTRA AÇÃO PENAL E ENVOLVIDO MAIS DE UMA VEZ EM CRIMES VIRTUAIS. MUDANÇA DE ENDEREÇO NÃO INFORMADA AO JUÍZO COMPETENTE. PEDIDO DE TRANSFERÊNCIA PARA PRESÍDIO PRÓXIMO À RESIDÊNCIA DA FAMÍLIA. JUÍZO DE EXECUÇÕES PENAIS. ORDEM DENEGADA. 1. Cuida-se de HABEAS CORPUS, com pedido liminar, impetrado em favor de RAUL BEZERRA DE ARRUDA JÚNIOR, apontando como autoridade coatora o Juiz Federal da 6ª Vara Federal da Seção Judiciária da Paraíba por ter indeferido o pedido de liberdade provisória, nos autos do processo n.º 0001537- 02.2014.4.05.8201, face à sentença penal condenatória proferida nos autos da Ação Penal n.º 2006.82.01.001114-6, instaurada para apurar a prática dos delitos tipificados nos artigos 1º, VII, c/c parágrafo 2º, inc. I, da Lei n.º 9.613/98, e nos Arts. 288 e 155, parágrafo 4º, inc. II e IV, do Código Penal. 2. Depreende-se dos autos que o paciente, juntamente com outros cinco acusados, em liame subjetivo permanente, formaram uma quadrilha visando ao furto sistemático de contas bancárias, mediante a utilização de programas preparados para invadir e subtrair contas bancárias pela internet, o que configuraria, em tese, os tipos penais previstos nos artigos 155, parágrafo 4º, inciso II e IV, e 288, ambos do Código Penal, no artigo 10 da Lei n. 9.296/96, no artigo 10 da Lei Complementar n. 105/2001 e no artigo 1º, inciso VII, c/c parágrafo 2º, inciso I, da Lei n. 9.613/98. 3. O impetrante sustenta, em síntese, que a decisão de indeferimento do pedido de liberdade provisória carece de fundamentos concretos e sem qualquer alicerce para a manutenção da segregação cautelar do paciente. Pugna, pois, pela concessão da ordem assegurando-lhe o direito de responder a todos os atos do processo em liberdade até o seu trânsito em julgado, ou, na remota impossibilidade, a imediata transferência do paciente para um presídio próximo à localidade da residência de sua família situada em Parnamirim/RN. 4. Afastada a alegação de

> nulidade do ato judicial de negativa do direito de apelar em liberdade, porquanto satisfatoriamente fundamentado pelo juízo a quo na parte dispositiva da sentença condenatória. Excerto da sentença transcrito. 5. Conforme se infere da parte dispositiva da sentença condenatória, o paciente não se inibiu de continuar a prática delitiva tendo sido preso novamente em cumprimento à determinação do Juízo da Comarca de Pombal-PB nos autos do Processo n.º 1921-53.2012.815.0301, além de ter-se envolvido mais de uma vez em crimes virtuais. Consta, ainda, o registro de que o paciente não foi localizado pela Polícia Federal nos endereços indicados em Campina Grande/PB. 6. A não comunicação de mudança de endereço ao juízo competente, bem como a reiteração das condutas delituosas, revela a inadequação e insuficiência das medidas cautelares alternativas à prisão previstas no art. 319 do CPP. 7. Considerando que inexistem elementos nos autos suficientes à análise do pedido de transferência do paciente para um presídio próximo à localidade da residência de sua família (Parnamirim/RN), cabe ao Juízo de Execuções Penais do Rio Grande do Norte apreciar tal pretensão. Ordem de habeas corpus denegada em consonância com o parecer ministerial. (TRF-5 - HC: 00093902720144050000 AL, Relator: Desembargador Federal José Maria Lucena, Data de Julgamento: 15/01/2015, Primeira Turma, Data de Publicação: 22/01/2015. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/trf-5/24828946. Acesso em: 22 jul. 2022).

Logo, trata-se de crime virtual cujo criminosos foram devidamente enquadrados na prática de furto qualificado, sendo irrelevante a prática do crime ter sido no ambiente virtual, com fundamentação nos dispositivos presentes no Código Penal.

Abaixo outra jurisprudência sobre crime praticado no âmbito da internet, mais especificamente de calúnia, difamação e injúria majoradas, com aplicação dos respectivos dispositivos penais:

> PROCESSUAL PENAL. RECURSO ORDINÁRIO EM HABEAS CORPUS. CALÚNIA, DIFAMAÇÃO E INJÚRIA MAJORADAS. ALEGAÇÃO DE INÉPCIA DA INICIAL. FALTA DE INDICAÇÃO DO LOCAL DOS FATOS. INCOMPETÊNCIA TERRITORIAL. PRECLUSÃO. EQUÍVOCO NA CAPITULAÇÃO JURÍDICA. NÃO OCORRÊNCIA. RÉU SE DEFENDE DOS FATOS. INVIABILIDADE DE INCURSÃO NO ACERVO PROBATÓRIO. NULIDADES. PRECLUSÃO PARA APRESENTAR RESPOSTA À ACUSAÇÃO. INOCORRÊNCIA. CERCEAMENTO DE DEFESA. NOMEAÇÃO DE DEFENSOR AD HOC SEM ANUÊNCIA DA PARTE. NÃO VERIFICAÇÃO. INTELIGÊNCIA DO ART. 44, DO CPC/1973. MATÉRIAS JÁ EXAMINADAS. REITERAÇÃO DE PEDIDO. RECURSO ORDINÁRIO DESPROVIDO. I - Os crimes contra a honra praticados pela internet são classificados como formais, ou seja, a consumação se dá no momento de sua prática, independente da ocorrência de resultado naturalístico, de forma que a competência deve se firmar de acordo com a regra do art. 70 do CPP - "A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução". II - A simples divulgação do conteúdo

> supostamente ofensivo na internet já é suficiente para delimitação da competência, sendo aquela do lugar em que as informações são alimentadas nas redes sociais, irrelevante o local do provedor. Precedentes. III - A competência territorial possui natureza relativa, motivo pelo qual deve ser arguida na primeira oportunidade em que a parte se manifesta nos autos, sob pena de preclusão. IV - Não há que se falar em inépcia da denuncia que atende o disposto no art. 41 do CPP, narrando de forma suficiente as condutas em tese praticadas pelo recorrente, possibilitando o amplo exercício do seu direito de defesa. V - Para concluir acerca da ocorrência de concurso formal próprio ou impróprio, seria necessário aprofundado exame do acervo probatório, o que é inviável em sede de recurso ordinário. VI - Quanto à alegada nulidade por ausência de resposta à acusação, tal matéria foi apreciada no julgamento do RHC n. 74047, onde constou: "Ora, o que se aventa, in casu, como nulidade, nada mais é do que estratégia equivocada e malsucedida da defesa, a qual optou por requerer, no último dia do prazo para apresentação da resposta à acusação, a renovação deste, em função de eventual deferimento de designação de audiência de reconciliação ou, alternativamente, a oitiva das testemunhas que arrolava." VII - No mesmo voto ficou assentado que "por opção da defesa, não houve a invocação das teses que possibilitariam a absolvição sumária da recorrente, nos termos do art. 397, do CPP, não havendo se falar em prejuízo, pois pode ser reconhecida como resposta à acusação a mera apresentação do rol de testemunhas, nos termos da legislação que rege o tema." VIII - Em relação ao alegado cerceamento do direito de nomear advogado, constou no mesmo decisum: "ex vi do art. 3º, do CPP, aplicava-se ao processo penal o disposto no art. 44, do CPC/1973, que expressamente afirmava:" A parte, que revogar o mandato outorgado ao seu advogado, no mesmo ato constituirá outro que assuma o patrocínio da causa"(Precedente). Não tendo sido tomada tal providência, era dever da magistrada processante designar defensor dativo para o ato, nos termos do art. 263, do CPP." IX - Vige no sistema processual penal o princípio da lealdade, da boa-fé objetiva e da cooperação entre os sujeitos processuais, não sendo lícito à parte arguir vício para o qual concorreu em sua produção, sob pena de se violar o princípio de que ninguém pode se beneficiar da própria torpeza - nemo auditur propriam turpitudinem allegans. X - O recorrente não logrou apontar e tampouco demonstrar o prejuízo, elemento essencial para o reconhecimento da suposta ilegalidade, nos termos do art. 563 do CPP - pas de nullitte sans grief. Recurso ordinário desprovido. (STJ - RHC: 77692 BA 2016/0283021-4, Relator: Ministro FELIX FISCHER, Data de Julgamento: 10/10/2017, T5 - QUINTA TURMA, Data de Publicação: DJe 18/10/2017. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stj/514506345/inteiro-teor-514506355. Acesso em: 30 jul. 2022).

Assim, trata-se de mais uma ocorrência de crime contra a honra praticado no ambiente virtual. Esse é um dos crimes mais frequentes e com elevada incidência, já sendo extremamente relevante a sua prática no âmbito virtual, visto que a ofensa possui potencial lesivo consideravelmente maior, considerando a facilidade de propagação e reprodução da informação.

Ainda sobre os crimes virtuais, segue mais uma jurisprudência sobre crime praticado no ambiente virtual, neste caso se tratando de fraude e roubo de dados bancários:

> CONTRATO BANCÁRIO. Ação para condenar ao pagamento de indenização por danos materiais. Procedência. Alegação de ação de fraudador para apropriação de informações bancárias secretas e realização de transferências de valores não autorizadas. Considerando-se a veracidade dos fatos narrados, tem-se que a autora teria sido vítima do golpe. Instalação de programa de computador responsável pela captação de dados. Digitação de senha e sequência numérica em programa de computador não oficial. Ausência de relação de causalidade entre o ato praticado pelos terceiros e a atividade desenvolvida pela ré. Culpa exclusiva da vítima. Excludente de responsabilidade. Ausência de falha nos serviços prestados. Inexistência do dever de indenizar. Improcedência. Sentença modificada. Recurso provido. (TJ-SP 10993252920178260100 SP 1099325-29.2017.8.26.0100, Relator: Sebastião Flávio, Data de Julgamento: 02/07/2018, 23ª Câmara de Direito Privado, Data de Publicação: 02/07/2018)

Nesse caso, observou-se que a fraude ocorreu por culpa exclusiva da vítima, não sendo cabível a responsabilização da instituição bancária. Os criminosos invadiram o computador por meio de programas específicos que captaram os dados sensíveis do usuário. Cabe ressaltar que os usuários da rede que não possuem vastos conhecimentos sobre informática estão muito propensos a se tornarem vítimas desses crimes, eis que os agentes já evoluíram suas técnicas e recursos de modo a facilmente ludibriarem seus alvos.

Por fim, segue abaixo jurisprudência interessante relativa ao delito de posse de material pornográfico infanto-juvenil:

> HABEAS CORPUS Nº 413.069 - SP (2017/0208680-6) RELATOR: MINISTRO JOEL ILAN PACIORNIK IMPETRANTE: DEFENSORIA PÚBLICA DA UNIÃO ADVOGADO: DEFENSORIA PÚBLICA DA UNIÃO IMPETRADO: TRIBUNAL REGIONAL FEDERAL DA 3A REGIÃO PACIENTE: MICHAEL LEME DE QUEIROZ DECISÃO Cuida-se de habeas corpus substitutivo de recurso próprio, com pedido de liminar, impetrado em benefício de MICHAEL LEME DE QUEIROZ, contra acórdão do Tribunal Regional Federal da 3ª Região (APC n. 2016.61.14.002516-6). Consta dos autos que o paciente foi condenado em primeiro grau pela prática dos crimes do 20 arts. 241-A e 241-B, do Estatuto da Criança e do Adolescente c.c. art. 69 do Código Penal, à pena de 4 (quatro) anos de reclusão, em regime aberto, consistentes em prestação de serviços à comunidade e prestação pecuniária. O Tribunal Regional Federal da 3ª Região, por sua vez, negou provimento ao recurso defensivo e deu parcial provimento ao recurso ministerial, conforme ementa a seguir transcrita: DIREITO PENAL. PROCESSO PENAL APELAÇÕES CRIMINAIS. PORNOGRAFIA INFANTO-JUVENIL. LEI 8.069/90. ARTIGOS 241-A E 241-B. PROGRAMA DE COMPARTILHAMENTO DE DADOS. USO.

> COMPETÊNCIA. JUSTIÇA FEDERAL. DOLO CARACTERIZADO NO COMPARTILHAMENTO DOS ARQUIVOS ILÍCITOS. AUTORIA E MATERIALIDADE INCONTROVERSAS. ABSORÇÃO. INOCORRÊNCIA NO CASO CONCRETO. CONDENAÇÃO MANTIDA. DOSIMETRIA. ALTERAÇÕES. 1. Réu flagrado em posse de acervo de fotografias e vídeos de pornografia infantojuvenil, acervo este armazenado digitalmente em discos rígidos de sua propriedade. Teria, ainda, compartilhado arquivo do mesmo teor anteriormente. [...] Em outros termos: ao disponibilizar arquivos de conteúdo pornográfico infanto-juvenil em servidor mundialmente acessível, o que há é a disponibilização/divulgação de pornografia infanto-juvenil além das fronteiras nacionais, o que torna claro seu caráter transnacional. [...] 3. Por sua vez, a constatação da internacionalidade do delito demandaria apenas que a publicação do material pornográfico tivesse sido feita em "ambiência virtual de sítios de amplo e fácil acesso a qualquer sujeito, em qualquer parte do planeta, que esteja conectado à internet" e que "o material pornográfico, envolvendo crianças ou adolescentes tenha estado acessível por alguém no estrangeiro, ainda que não haja evidências de que esse acesso realmente ocorreu" [...] Publique-se. Intime-se. Brasília (DF), 23 de fevereiro de 2018. (STJ - HC: 413069 SP 2017/0208680-6, Relator: Ministro Joel Ilan Paciornik, Data de Publicação: DJ 28/02/2018)

Como pode ser visto, foi também constatada a possibilidade de reconhecimento da transnacionalidade dos crimes cibernéticos nesses casos, conforme dispõe o SJT em sua decisão, diante da publicação do conteúdo em sites de repercussão e acessos internacionais. Cabe observar que a referida jurisprudência se pautou na proteção da liberdade sexual e dignidade infantis, aplicando os dispostos nos Arts. 241-A e 241-B do Estatuto da Criança e do Adolescente, bem como na questão do expressivo agravamento do crime por ser cometido no ambiente público virtual.

CONCLUSÃO

O presente trabalho buscou refletir acerca da aplicação dos dispositivos penais aos crimes cibernéticos no âmbito do ordenamento jurídico brasileiro, bem como analisar o surgimento de novos institutos penalizadores mais específicos, com intuito de punir e coibir tais práticas, levando em consideração a sua eficiência prática.

Após uma breve ambientação histórica e definição desses delitos, foi possível estudar o modo com que a internet vem crescendo e se desenvolvendo, e observar o desenvolvimento dos direitos e garantias individuais no ambiente do ciberespaço. Foi constatado que o Brasil ainda é inseguro em relação à criminalidade cibernética, tanto em matéria legislativa quanto no tratamento oferecido aos crimes virtuais, e por mais que as leis vigentes tratem de alguma maneira a matéria exposta, o ordenamento jurídico ainda carece de inovações no seu diploma penal e processual penal, conforme foi exposto.

Ademais, foi possível realizar um exame crítico dos ilícitos virtuais, de modo a explorar as especificidades de tais práticas, assim como as inovações legislativas surgidas a partir da demanda por regulamentação das relações na rede. Com base na pesquisa bibliográfica, conclui-se que há consideráveis esforços para acompanhar a crescente incidência de crimes no âmbito da internet, mas que ainda não são suficientes para trazer soluções adequadas. Destaca-se como exemplo a criação das delegacias especializadas, que representam apenas um primeiro passo na direção certa, visto que ainda carentes de estrutura e recursos que possibilitem torna-las instituições eficientes na repressão e persecução penal dessas infrações.

Por fim, foram demonstrados, por meio de estudo exploratório e levantamento bibliográfico, os princípios constitucionais e as demais normas pertinentes, assim como os entendimentos doutrinários e jurisprudenciais cabíveis ao tema, estes que serviram de base para a investigação e análise crítica do Direito Digital e dos crimes virtuais. Foi realizada também, a perquirição dos delitos cibernéticos à luz do Direito Penal e Processual Penal brasileiro, apreciando as peculiaridades que tornam essas infrações difíceis de serem investigadas, mas relativamente fáceis de serem cometidas, demonstrando as dificuldades enfrentadas pelos

legisladores, com relação à normatização e definição, e dos órgãos de polícia judiciária, com relação à investigação e repressão dessas violações.

REFERÊNCIAS

ALVES, Gustavo Alberto. **Segurança da informação: Uma visão inovadora da gestão**. 1ª ed. – São Paulo: Ciência Moderna, 2006.

ANDRION, Roseli; YUGE, Claudio. **História da segurança virtual: a origem do antivírus de computador**. 2021. Disponível em: https://canaltech.com.br/seguranca/historia-da-seguranca-virtual-a-origem-do-antivirus-de-computador-197745/. Acesso em: 17/07/2022.

ARENDT, Hannah. **A condição humana.** 10ª ed. Rio de Janeiro: Forense Universitária, 2005.

BACH, Sirlei Lourdes. **Contribuição do hacker para o desenvolvimento tecnológico da informática**. Tese (Mestrado em Ciência da Computação) – Programa de Pós-Graduação em Ciência da Computação, Universidade Federal de Santa Catarina. Florianópolis, p. 121. 2001.

BARRETO, A. G. B.; BRASIL, B. S. **Manual de investigação cibernética à luz do Marco Civil da Internet**. São Paulo: Brasport, 2016.

BELTRÃO, Silvio Romero. **Direito da personalidade à intimidade.** 2012. Disponível em: http://www.tjpe.jus.br/documents/33154/34767/cap09.pdf/04061934-de43-437e-a2a4-9a68947dafa0. Acesso em: 29/10/2022.

BEZERRA, Juliana; **Revolução Industrial**. 2013. Disponível: https://www.todamateria.com.br/revolucao-industrial/. Acesso em: 12/07/2022.

BRANCO, Dácio Castelo; YUGE, Claudio. **História da segurança virtual: a origem do vírus de computador**. 2021. Disponível em: https://canaltech.com.br/seguranca/origem-do-virus-de-computador-197667/. Acesso em: 13/07/2022.

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

BRASIL. **Decreto-Lei nº 2.848, de 07 de dezembro de 1940**. Código Penal. Diário Oficial da União, Rio de Janeiro, 31 de dezembro de 1940.

BRASIL. **Lei nº. 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Diário Oficial da União, Brasília, 3 de dezembro de 2012.

BRASIL. **Lei nº. 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, 24 de abril de 2014.

BRASIL. **Lei nº 13.709 de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, 15 de agosto de 2018.

BRASIL. **Lei nº 14.155 de 27 de maio de 2021**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela internet; e o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), para definir a competência em modalidades de estelionato. Diário Oficial da União, Brasília, 28 de maio de 2021.

BRASIL. **Medida provisória nº 869, de 27 de dezembro de 2018**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Diário Oficial da União, Brasília, 28 de dezembro de 2018.

BRASIL. Supremo Tribunal de Justiça. **Recurso especial Nº 1117633/RO, Relator: Ministro Herman Benjamin**. Brasília, 09 de março de 2010. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/8569044/recurso-especial-resp-1117633-ro-2009-0026654-2/inteiro-teor-13668131. Acessado em: 17/07/2022.

BRASIL. Superior Tribunal de Justiça. **Justiça usa Código Penal para combater crime virtual.** Disponível em: https://stj.jusbrasil.com.br/noticias/234770/justica-usa-codigo-penal-para-combater-crime-virtual. Acesso em: 20/10/2022.

BRASIL. Supremo Tribunal Federal. Recurso Extraordinário 756.917. Relator: Min. Luiz Fux. – Primeira Turma. **Diário de Justiça Eletrônico,** 19 de novembro de 2013. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stf/24655778/inteiro-teor-112141306. Acesso em: 20/07/2022

BRASIL. Tribunal Regional Federal, Região 5. Furto qualificado através da rede mundial de computadores. Relator: Desembargador Federal José Maria Lucena. **Diário de Justiça Eletrônico,** 22 de janeiro de 2015. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/trf-5/24828946. Acesso em: 22/07/2022.

BRASIL. Superior Tribunal de Justiça**. Habeas Corpus 77692 BA 2016/0283021**. Relator: Ministro FELIX FISCHER, Data de Julgamento: 10/10/2017, T5 - QUINTA TURMA, Data de Publicação: DJe 18/10/2017. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stj/514506345/inteiro-teor-514506355. Acesso em: 30/07/2022.

BROOKSHEAR, J. Glenn. **Ciência da Computação: Uma visão abrangente**. 11ª ed. – Porto Alegre: Bookman, 2013.

BURÉGIO, Fátima. **Pornografia da Vingança:** você sabe o que é isto? 2015. Disponível em: https://ftimaburegio.jusbrasil.com.br/artigos/178802845/pornografia-da-vinganca-voce-sabe-o-que-e-isto. Acesso em: 11/10/2022.

CALDAS, Pedro Frederico, **Vida privada, liberdade de imprensa e dano moral**. São Paulo: Saraiva, 1997.

CAPEZ, Fernando. **Curso de direito penal 3.** 15 ed. São Paulo: Saraiva, 2017.

CARNEIRO, Adeneele Garcia. **Crimes virtuais:** elementos para uma reflexão sobre o problema na tipificação. Âmbito Jurídico, Rio Grande, XV, n. 99, abr. 2012. Disponível em: <http://www.ambito-juridico.com.br/site/?n_link=revista_. Acesso em: 11/10/2022.

CASTRO, A. L. C. de; SYDOW, S. T. **Exposição pornográfica não consentida na Internet:** da pornografia de vingança ao lucro. Belo Horizonte: D'Plácido, 2019. p. 134-136. Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_boletim/bibli_bol_2006/RTrib_n.959.02.PDF. Acesso em: 15/10/2022.

CONTE, Christiany Pegorari. **Jurisdição e competência nos crimes informáticos.** Revista Brasileira de Meio Ambiente Digital e Sociedade da Informação, São Paulo, 2014.

CONVENÇÃO SOBRE O CIBERCRIME. Budapeste, 2001. Disponível em: https://www.safernet.org.br/site/sites/default/files/Convencao-sobre-o-Cibercrime.pdf. Acesso em: 15/11/2022.

CORRÊA, Gustavo Testa**. Aspectos jurídicos da Internet**. 5ª Ed. São Paulo: Saraiva, 2010.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais.** São Paulo: Saraiva, 2011, p. 48.

DAMÁSIO DE JESUS apud ARAS, Vladmir. **Crimes de informática: Uma nova criminalidade**. Disponível em: http://jus.com.br/artigos/2250/crimes-de-informatica. Acesso em 13/09/2022.

DIAS, Maria Berenice. **A Lei Maria da Penha na Justiça.** Disponível em: <http://www.mariaberenice.com.br/uploads/17__a_lei_maria_da_penha_na_justi%E7a.pdf >. Acesso em: 18/10/2022.

DINIZ, Maria Helena. **Curso de Direito Civil Brasileiro, 7° volume: responsabilidade civil**. 21. ed. São Paulo: Saraiva, 2007.

DISTRITO FEDERAL. Tribunal de Justiça. Embargos de Declaração nº 07183442320178070001. Dever da Instituição Financeira de Provar a Regularidade das Operações. Relator: JOSAPHÁ FRANCISCO DOS SANTOS. **Diário da Justiça Eletrônico,** 11 de abril de 2018, 5ª Turma Cível. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-df/899812310/inteiro-teor-899812974. Acesso em: 30/07/2022.

ELMASRI, Ramez; NAVATHE, Shamkant B. **Sistemas de bancos de dados**. 6ª ed. São Paulo: Addison Wesley, 2011.

FEITOSA JR, Alessandro; SILVA, Victor Hugo. **Empresas vítimas de ransomware precisam avisar sobre ataque? Quem investiga? Veja perguntas e respostas**. G1, 28 de setembro de 2021. Disponível em: https://g1.globo.com/tecnologia/noticia/2021/09/28/empresas-vitimas-de-ransomware-

precisam-avisar-sobre-ataque-quem-investiga-veja-perguntas-e-respostas.ghtml. Acesso em 28/09/2022.

FERREIRA, Ivette Senise. A criminalidade informática. In: DE LUCCA, Newton; SIMÃO FILHO, Adalberto (Co-ord.). **Direito & internet: aspectos jurídicos relevantes**. São Paulo: Quartier Latin, 2008, v.2. p. 213.

FERREIRA, Ivette Senise. **Direito & Internet: Aspectos Jurídicos Relevantes**. 2 ª ed. – São Paulo: Quartier Latin, 2005, p. 261.

FONSECA, J. J. S. **Metodologia da pesquisa científica**. Fortaleza: UEC, 2002. Apostila.

GABRIEL, Martha. **Marketing na Era Digital**. São Paulo: Novatec Editora, 2010, p. 83.

GIL, A. C. **Como elaborar projetos de pesquisa**. São Paulo, SP: Atlas, 2002.

GRECO, Rogério**. Curso de Direito Penal.** 13. ed. Rio de Janeiro: Impetus, 2016.

GRECO, Rogério. **Curso de Direito Penal:** parte geral. Volume I: 19. ed. – Niterói, RJ: Impetus, 2017.

INELLAS, Gabriel Cesar Zaccaria de. **Crimes na internet.** São Paulo: Juarez de Oliveira, 2006.

INELLAS, Gabriel Cesar Zaccaria de. **Crimes na internet.** São Paulo: Juarez de Oliveira, 2004.

JESUS, Damásio E. de. **Código penal anotado**. 11. ed. São Paulo: Saraiva, 2001.

JESUS, Damásio E. de**. Direito penal – Parte Geral**. Vol. 1. São Paulo: Saraiva: 2003.

JESUS, Damásio E. de; MILAGRE, José Antônio. **Marco Civil da Internet: comentários à Lei n. 12.965/14**. São Paulo: Saraiva, 2014.

KASPERSKY. **Proteção contra ameaças de primeira classe**. 2022. Disponível em: https://www.kaspersky.com.br/blog/top3-awards-2021/19259/. Acesso em: 27/09/2022.

LUCAS, Izalci. **PROJETO DE LEI Nº ....., DE 2020**. Distrito Federal, 2020. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=8889742&ts=1600958354757&disposition=inline. Acesso em 15/11/2022.

MACHADO, F. N. R. **Bancos de Dados: Projeto e Implementação**. São Paulo: Ed. Erica 2004.

MACHADO, N. J. **Epistemologia e Didática – as concepções de conhecimento e inteligência e a prática docente**. São Paulo: Cortez, 2002.

MANCE, Euclides André. **A revolução das redes: a colaboração solidária como uma alternativa pós-capitalista à globalização atual**. Petrópolis, RJ: Vozes, 1999.

MENDES, Maria Eugenia Gonçalves; VIEIRA. Natália Borges. **Os crimes cibernéticos no ordenamento jurídico brasileiro e a necessidade de legislação específica.** 2012. Disponível em: http://www.gcpadvogados.com.br/artigos/os-crimes-ciberneticos-no-ordenamento-juridico-brasileiro-e-a-necessidade-de-legislacao-especifica-2. Acesso em: 18/10/ 2022.

PISA, Pedro. **O que é IP?**. 2016. Disponível em: http://www.techtudo.com.br/artigos/noticia/2012/05/o-que-e-ip.html. Acesso em: 20/10/2022.

POSSEBON, Samuel; YUGE, Claudio. **10 anos do decálogo da Internet: os princípios ainda estão atuais?**. 2019. Disponível em: https://teletime.com.br/05/06/2019/10-anos-do-decalogo-da-internet-os-desafios-atuais-e-futuros/. Acesso em: 05/10/2022.

ROCHA, Carolina Borges (2013). **A evolução criminológica do Direito Penal:** aspectos gerais sobre os crimes cibernéticos e a Lei 12. 737/2012. Disponível em: http://www.amab.com.br/fileadmin/user_upload/A_evolucao_criminologica_do_Direito_Penal.pdf. Acesso: 20/10/2022.

SÃO PAULO. Tribunal de Justiça. Apelação Cível nº 1001965-91.2018.8.26.0704. Ação de obrigação de fazer contra Facebook; Twitter; Google; Rede Record TV e Universo Online S/A UOL. Apelante: U.O.S.A., F.S.O. do B. LTDA e T.B.R. de I. LTDA. Apelado: M.C.L.S. de L.P. Relator: Edson Luiz de Queiroz, São Paulo, 3 de agosto de 2021. **Jusbrasil.** Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-sp/1258146701/inteiro-teor-1258146722. Acesso em: 27/07/2022.

SÊMOLA, Marcos. **Gestão da segurança da informação: uma visão executiva**. Rio de Janeiro: Elsevier, 2003.

SILBERSCHATZ, Abraham; KORTH, Henri F, & SUDARSHAN S. **Sistemas de Banco de Dados**. São Paulo: Makron Books, 1999.

SILVA NETO, Manoel Jorge e. **Curso de direito constitucional.** 6. ed. Rio de Janeiro: Lumen Juris, 2013.

TABOSA, Bianca M. Batista et al. **A psicopatia em sua dimensão virtual: um olhar acerca do fenômeno baleia azul**. Revista Eletrônica de Direito da Faculdade Estácio do Pará, v. 4, n. 5, 2017.

TOMAZ, Kleber. **Governo de SP inaugura divisão policial com delegacias especializadas no combate a crimes cibernéticos**. G1, 2020. Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2020/12/19/governo-de-sp-inaugura-divisao-policial-com-delegacias-especializadas-no-combate-a-crimes-ciberneticos.ghtml. Acesso em: 20/10/2022.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos:** ameaças e procedimentos de investigação. 2. ed. São Paulo: Brasport, 2013.