CIBERCRIMINALIDADE: UMA RELEITURA ACERCA DO "*MODUS OPERANDI*"

Danielly Kellen Arruda da Silva[1]
Jorge Heleno Costa[2]

RESUMO

Com o crescimento de diversos recursos tecnológicos surgiram novas formas de comportamento delituoso, os criminosos se adaptaram ao meio virtual e surgiram diversificadas formas de cometimentos de delitos convencionais. No entanto, é possível questionar se o ordenamento jurídico é capaz de acompanhar todo esse avanço. Diante deste contexto, o presente artigo visa examinar a nova atuação dos criminosos pelo meio virtual, com ênfase em suas características, conceito e a modificação do *modus operandi* do cibercrime. Além disso, pretende verificar, também, se houve avanços legislativos quanto à tipificação dos cibercrimes. A metodologia utilizada neste trabalho, como suporte de seu desenvolvimento, procederá por meio de uma pesquisa exploratória de cunho bibliográfico e documental. Para tanto, foi necessária a utilização de documentos públicos como leis, informes estatísticos, informações disponíveis em sites, livros e artigos.

PALAVRAS-CHAVES: Direito Penal, Crimes Cibernéticos, *Modus Operandi,* Internet.

INTRODUÇÃO

O avanço tecnológico trouxe consideráveis benefícios, unindo a população mundial frente a aparelhos mediante a possibilidade de acessibilidade que estes apresentaram.

Nas últimas décadas, a população está constantemente conectada ao meio virtual por meio de celulares, notebooks, tablets e outros dispositivos conectados à rede mundial de computadores (internet). O objetivo desta crescente conexão é realizar praticamente todas as atividades do dia-a-dia, seja para o trabalho, acesso

[1] Graduanda do curso de Direito no Centro Universitário Presidente Tancredo de Almeida Neves - UNIPTAN. E-mail: daniellykellen@yahoo.com.br

[2] Professor do curso de Direito no Centro Universitário Presidente Tancredo de Almeida Neves - UNIPTAN. E-mail:jorge.costa@uniptan.edu.br

às redes sociais, obtenção de informação, acesso ao e-mail, operações bancárias, dentre outras.

Com a decretação da pandemia da COVID-19 aumentou, exponencialmente, o acesso ao meio virtual devido ao isolamento vivenciado a partir de março de 2020, já que houve o implemento compulsório do *home office* e *home study.* Dessa forma, o ambiente virtual se tornou um meio de poderosa comunicação e informações, porém, a abrangência dessa evolução trouxe situações negativas para seus usuários.

É indiscutível que o meio virtual se tornou um veículo fundamental para as pessoas, contudo o que foi criado para promover maior interatividade entre as pessoas, abriu espaço para aquelas mal intencionadas que modificam e aprendem novas formas de praticar algum ato ilícito.

No meio virtual acontecem diversos tipos de crimes e os criminosos usam as mais variadas estratégias para atuar e se adaptarem à tecnologia. É possível verificar essa problemática quando se percebe uma população receosa e com sensação de impunidade aos cibercrimes.

Os cibercriminosos têm várias modalidades para cometer seus crimes, com inúmeras formas estratégicas de atuação, sendo cada vez mais aperfeiçoados e constantes. A nebulosidade no meio virtual, mediante a não compreensão dos riscos e dos desconhecimentos tecnológicos, evidencia a facilidade para a prática criminosa numa diversidade considerável.

Presume-se que a evolução tecnológica é significativamente superior à do legislador, tendo em vista que os cibercrimes se multiplicam cotidianamente, não conseguindo o legislador, assim, acompanhar tal evolução tecnológica e fazer com que a legislação evolua no mesmo passo, o que dificulta de certa forma a averiguação e punição do cibercriminoso.

O Código Penal quando confrontado com delitos de natureza cibernética, deixa bem claro suas deficiências, já que a Parte Especial do referido Código data de 1940, época em que os sistemas computadorizados sequer tinham dado surgimento e mesmo as alterações legislativas posteriores não cuidam de maneira efetiva, a respeito dessa matéria.

Este artigo foi desenvolvido com o objetivo de analisar os crimes cometidos pelo meio virtual e evolução do seu *modus operandi*, assim como a não punição, em virtude da falta de evolução das normas jurídicas no Brasil.

Para isso, a metodologia utilizada no presente trabalho, como suporte de seu desenvolvimento, procederá por meio de uma pesquisa exploratória, de cunho bibliográfico e documental, realizadas pesquisas a artigos disponíveis online, livros doutrinários, legislações vigentes e outros materiais para complementar.

1 EVOLUÇÃO TECNOLÓGICA

Perante os avanços tecnológicos nos últimos 10 anos ficam evidentes as mudanças significativas e aumento das facilidades experimentadas por todos os seres humanos, como por exemplo, a comunicação e o compartilhamento de dados, potencializando a era digital.

Nas palavras de Deslandes e Arantes (2017, p. 175):

> Em um mundo contemporâneo, a internet é hoje ferramenta primordial que proporciona novos moldes de relacionamento social. Nos dias atuais é mecanismo de primeira necessidade, pois, se vende, se compra, fecham-se negócios, usando a internet. Pessoas se conhecem e se relacionam pelas redes sociais, em uma velocidade que talvez jamais fosse mensurada há uma década. Neste mesmo contexto e velocidade crescem também os crimes virtuais, principalmente os relacionados às redes sociais. Tais crimes aumentaram muito, devido à facilidade encontrada para praticá-lo, onde muitas informações pessoais estão disponíveis na rede. Assim, os criminosos coletam dados e informações privilegiadas para extorquir ou simplesmente prejudicar o outro, causando prejuízos moral e financeiros.

Entretanto, toda essa evolução não aconteceu por mero acaso. O computador, juntamente à internet, passou por diversas transformações, levando-se em consideração que antes os equipamentos que ocupavam uma sala tiveram seu tamanho extremamente diminuído.

A internet, por sua vez, surgiu durante a Guerra Fria. Os EUA com enorme temor de um ataque nuclear da União Soviética e de modo a resguardar informações e arquivos e manter as comunicações entre as bases, deu origem a ARPANET (*Advanced Research Projects Agency)*, desenvolvida por cientistas

ligados ao Departamento de Defesa norte-americano, sendo somente de uso militar até então (ALVES, 2020, p. 17-20).

Desta forma, destaca Sydow (2015, p. 31):

> Assim, a ideia foi a de difundir a informação sem que houvesse somente um centro estratégico frágil, que, atacado, levaria a um caos desenvolvimentista, permitindo-se que a informação trafegasse mesmo que tivesse havido perda de um dos núcleos tecnológicos. Pode-se dizer, portanto, que a importância inicial da rede informática foi estratégica.

A ARPANET teve como objetivos principais o funcionamento em rede para casos de calamidades e a troca de informações rápidas e de forma segura entre bases militares, porém, nunca se imaginou que a internet cresceria de forma colossal a ponto de transcender os objetivos iniciais.

Dessa forma, como todo esse avanço tecnológico, é evidente que o mundo está mais conectado, através de meios de comunicação rápido e com grande acervo de informações e dados pessoais, e isso trouxe grandes vulnerabilidades.

2 CRIMES CIBERNÉTICOS E O *MODUS OPERANDI*

Os crimes cibernéticos se separam das condutas praticadas no meio físico, pois têm natureza computacional e com alcance global. Diante disso, pode-se afirmar ser aquelas condutas ilícitas praticadas por pessoas físicas ou jurídicas valendo-se da tecnologia e meio virtual.

Além disso, segundo site Significados a expressão em latim *modus operandi* tem como significado literal “modo de operação”. No âmbito jurídico, o *modus operandi* se refere a como o crime é praticado pelo agente, determinando os atos para realização de certo crime com a sua consequente consumação, ou seja, identifica o perfil dos criminosos.

2.1 Classificação dos crimes cibernéticos

Há grande dificuldade em estabelecer e definir uma nomenclatura para os crimes cometidos por redes de dados. Porém, o termo mais utilizado no momento é

o cibercrime, que engloba as pessoas que fizeram uso de aparelhos eletrônicos de forma a acessar, manipular ou utilizar dados para fins ilícitos.

Nas palavras de Crespo (2015):

> Simplificando, pode-se dizer que os crimes digitais são tanto os crimes tradicionais, já previstos na legislação, contra os valores que tradicionalmente reconhecemos como merecedores de proteção, praticados com auxílio da mais moderna tecnologia, bem como as condutas ilícitas passíveis de penas que se voltem contra os sistemas informatizados e os dados.

Há diversos entendimentos doutrinários sobre a natureza jurídica e classificação dos crimes cibernéticos. Porém, neste artigo, será adotada a classificação de crimes cibernéticos como próprios e impróprios.

Os crimes cibernéticos próprios, também chamados puros, são aqueles onde as condutas atingem o próprio computador físico e seus componentes (*Hadware*) ou seu sistema operacional (*software*), ofendendo bens jurídicos informáticos (ALVES, 2020, p.38).

A título de exemplo de crimes cibernéticos próprios: invasão de dados armazenados em computador, interceptação de e-mails, introdução de *malwares* (aplicativo que adentra um sistema com intenção de repassar informações ou causar danos no sistema operacional do dispositivo eletrônico da vítima).

Já os crimes cibernéticos impróprios são aqueles em que a pessoas recorre ao meio tecnológico para cometer crimes já tipificados no Código Penal brasileiro, ou seja, faz uso da tecnologia para lesar bens jurídicos tradicionais por meio de outro *modus operandi*. Como exemplo: crimes contra a honra, ameaça, estelionato.

Conforme a linha de pensamento de Vianna (2001, p.38):

> Delitos informáticos impróprios são aqueles nos quais o computador é usado como instrumento para a execução do crime, mas não há ofensa ao bem jurídico da informatização automatizada.

Em suma, de forma geral os crimes cibernéticos podem ser considerados como outra forma de se praticar crimes antigos, só que utilizando do meio digital, eletrônico.

2.2 Os cibercriminosos e sua nova forma de atuação

Os cibercriminosos não têm um perfil específico ou padronizado, pois diversos crimes praticados no meio tecnológico não necessitam de grandes habilidades informáticas, como caluniar ou ameaçar em redes sociais. Mas, há práticas de cibercrimes em que a pessoa necessita de um certo conhecimento tecnológico, especialmente em condutas que envolvam programação (SYDOW, 2015, p.143).

Há inovação rotineira na prática de crimes cometidos no meio digital, com mais facilidade em ludibriar as vítimas e consumar o fato ilícito. Além da facilidade de se manterem anônimos, o que é vedado pela Constituição Federal de 1988, em seu art. 5º, inciso IX, tornando um ambiente propício para cometimento de crimes, além de dificultar sua identificação.

Na maioria dos crimes cometidos no meio virtual acaba se aproveitando da vulnerabilidade do aparelho.

Dentre os crimes em evidência, importante dar ênfase ao cibercrime denominado *phishing,* crime em ascensão no meio virtual, em que há um *modus operandi* característico do cibercriminoso e é analogamente comparado ao crime de estelionato.

O *phishing* é um roubo de dados pessoais, onde a forma de atuação da pessoa para obtenção desses dados se dá ao enviar e-mails fictícios com links que são remetidos a sites fraudulentos que passam por originais e confiáveis, a vítima acaba divulgando suas informações pessoais como dados de cartão de crédito, contas de bancos, dentre outros que possibilita ao cibercriminoso se utilizar de tais dados para uso de fins não autorizados, como compras, obtenção de empréstimos, etc.

Como pode se observar ao exemplo do *phishing,* crime cometido pelo meio virtual, é tratado análogo ao crime de estelionato, em que não tem a mesma forma de atuação ou seu *modus operandi* idêntico do estelionatário.

Ainda, segundo Vianna (2001, p.60), os sujeitos desenvolvedores de *malwares* e seu *modus operandi,* são classificados em:

> 1. CRACKERS DE SISTEMAS – piratas que invadem computadores ligados em rede.
> 2. CRACKERS DE PROGRAMA – piratas que quebram proteções de *software* cedidos a título de demonstração para

> usá-lo por tempo indeterminado, como se fossem cópias legítimas.
> 3. PHREAKERS – piratas especialistas em telefonia móvel ou fixa.
> 4. DESENVOLVEDORES DE VÍRUS, WORMS E TROJANS – programadores que criam pequenos *softwares* que causam algum dano ao usuário.
> 5. PIRATAS DE PROGRAMAS – indivíduos que clonam programas fraudando direitos autorais.
>
> 6.DISTRIBUIDORES DE WAREZ – *webmasters* que disponibilizam em suas páginas *softwares* sem autorização dos detentores dos direitos autorais.

Diante desses fatores, é importante frisar que os crimes cibernéticos são a contraparte dos crimes antigos e cibercriminosos cada dia mais inovam sua forma de atuação, com mais conhecimentos técnicos para consumação de crimes tradicionais ou para prática de novos delitos.

3 LEGISLAÇÃO BRASILEIRA ESPECÍFICA EM REFERÊNCIA DOS CRIMES CIBERNÉTICOS

A conjuntura legislativa brasileira, quando confrontada com crimes de natureza cibernética, deixa nítido suas deficiências, até mesmo porque o Código Penal é de 1940, ano em que nem se imaginaria tamanha tecnologia que é vivenciada no séc. XXI.

Em suma, importante frisar que há algumas normas que regulamentam crimes cibernéticos, porém, não de forma suficiente para englobar todas as condutas ilícitas no meio virtual.

3.1 A Convenção de Budapeste

A Convenção do Cibercrime do Conselho da Europa, conhecida como a Convenção de Budapeste, está vigente desde o ano de 2004 e é uma referência global. Foi o primeiro tratado internacional a abordar sobre o assunto de crimes cometidos na internet, além de referir, de forma especifica, à segurança de rede de computadores, fraude informática, violação de direitos autorais e pornografia infantil.

Objetivou-se estabelecer uma regulamentação e política comum entre os Estados Membros (países que adotaram o Tratado) e ações conjuntas para que haja

cooperação internacional em caso de crimes virtuais, em virtude da globalização delituosa. É subdividida em direito penal material (arts. 2º a 13), direito processual penal (arts. 14 a 22) e cooperação internacional (arts. 23 a 35).

O Brasil foi convidado a incorporar ao tratado em 2019, após diligências do Ministério da Justiça e Segurança Pública, quando foi manifestada a intenção de aderir ao aparato internacional. A adesão do Brasil à Convenção de Budapeste sobre crimes cibernéticos coincide com a intensa digitalização da vida e o inegável aumento de atividades criminosas cometidas online, inclusive a violação sistemática de direitos autorais.

Conforme Senna e Ferrari (2020):

> A demanda pela adesão do Brasil vem somar-se à lei 12.965/14 - o Marco Civil da Internet, visando suprir a carência por um marco equivalente na seara criminal que desse conta da delimitação de parâmetros de persecução penal para tais crimes que, por sua própria natureza, transcendem as fronteiras geográficas.

A Convenção de Budapeste tem grande importância em ser o primeiro tratado internacional sobre crimes virtuais e objetiva a cooperação entre os Estados-Membros ao se destinar em harmonizar os ordenamentos internos.

3.2 Marco Civil da Internet

A Lei nº 12.965/14 conhecida, também, como a Constituição da Internet, trouxe respostas legislativas para fortalecimento e reconhecimento de direitos perante a internet. Perante pressão popular para elaboração e aprovação de uma Lei que atendesse e enrijecesse as penas para os crimes cometidos na internet, resultou na aprovação da lei, objetivando suprir lacunas deixadas na normatização das leis anteriores.

Deve se avultar, que o Marco Civil “estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria “(Brasil, 2014).

De acordo com Alves (2020, p.108):

> Com a entrada em vigor do Marco Civil da Internet, a operação das empresas que atuam na internet passa a ser mais

> transparente, a proteção de dados pessoais e a privacidade dos usuários passam a ser garantidas por lei. Isso significa, por exemplo, que essas empresas que trabalham com os dados dos usuários com fins publicitários não poderão mais repassar suas informações para terceiros sem que haja o livre e expresso consentimento do usuário.

Apesar do Marco Civil da Internet ter objetivado projetar as demandas e evoluções da sociedade, não foi suficiente para combater as práticas ilícitas praticadas no meios virtuais, vindo a vigorar a Lei Geral de Proteção de Dados (LGPD) em 18 de setembro de 2020, como forma de proteção dos dados pessoais dos usuários, pois o mau uso desses dados podem gerar efeitos devastadores aos titulares.

3.3 Lei Carolina Dieckmann

A Lei 12.737/12 (BRASIL, 2021) foi criada após um crime contra a honra da atriz brasileira Carolina Dieckmann, que teve seu computador invadido por *crackers* (definição de *hackers* maliciosos) e copiaram suas fotos íntimas. Tal lei teve como objetivo principal a punição do indivíduo que cria e espalha vírus computacional e *malwares* a fim de furtar senhas.

A lei mencionada incluiu em nosso Código Penal os artigos 154-A e 154-B e alterou os artigos 266 e 298 (BRASIL, 1940). Sendo bem tutelado pelos artigos trazidos nessa lei a proteção à intimidade, direito constitucional.[3]

Com essa redação ficava a crítica mediante o fato que era necessário o mecanismo de proteção no sistema computacional, conforme mencionado “mediante violação indevida de mecanismos de segurança”.

Desta forma, a lei acabou restringindo a tipicidade da invasão de dispositivos informáticos em situações que haveria somente violação indevida caso estivesse presente um mecanismo de segurança, excluído os não dotados de ferramenta de proteção.

---

[3] “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.” (grifo nosso)

Cabe mencionar que o art. 154-A teve intenção de punir não somente os invasores, mas aqueles que facilitam o delito através de criação de programas. Além, da nova redação do art. 298 trazer a equiparação do cartão de crédito a um documento particular, de modo a punir o roubo de dados dos cartões de crédito e sua utilização indevida.

Insta salientar que a Lei 14.155/2021 modificou o art. 154- A, tornando-o mais rigoroso na punição e modificando a redação ao excluir a parte que menciona "mediante violação indevida de mecanismos de segurança" (BRASIL, 2021)[4], acabando com a discussão acerca da restrição da tipicidade e abrangendo todos os dispositivos.

Em suma, é evidente que o legislador promulgou a lei preocupado com a repercussão midiática e, consequentemente, com a pressão da opinião pública, no qual uma atriz brasileira teve imagens íntimas divulgadas, porém, deixou lacunas na interpretação da lei.

3.4 Lei Azeredo

A Lei Azeredo, apelido que faz alusão ao relator Eduardo Azeredo, promulgada juntamente com a Lei Carolina Dieckmann, objetivou a criação de repartições e equipes especializadas no combate a crimes cibernéticos ou sistema informatizado.

O projeto de lei 84/99, que após tornaria a Lei 12.735/2012, foi apelidada de "AI-5" devido alguns pontos controversos, sendo vetados antes da vigência. Devido a isso acabou sendo sancionada com reduzidas disposições.

O texto de lei aprovado determina que órgãos de polícia judiciária criem delegacias especializadas, conforme seu art. 4º[5], com a finalidade de combater os crimes cometidos digitais. Porém, a obrigação de criação de delegacias de combate

---

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

[5] Art. 4º. Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

a crimes cibernéticos não quer dizer que estas estão aptas e plenamente capacitadas para atendimento às vítimas desses crimes.

3.5 Lei Geral de Proteção de Dados Pessoais - LGPD

Lei recentemente promulgada, a fim de suprir lacunas de outras leis com o mesmo cunho legislativo, sendo o objetivo de regular o tratamento de dados pessoais nos meios digitais para proteção dos direitos fundamentais de liberdade e privacidade (ZANIOLO, 2021, p.643).

A Lei nº 13.709 promulgada em 14 de agosto de 2018, teve vigência na data 18 de setembro de 2018, vem como forma de proteger os dados pessoais no meio virtual para que não sejam usados de forma maliciosa. Contudo, é necessário que as empresas tenham o consentimento das pessoas para utilizar de seus dados pessoais compartilhados nos sites, além dos usuários terem garantido o direito de revogação do consentimento de utilização de seus dados (SANTIN, 2019).

Tal lei deve ser aplicada a pessoas jurídicas ou físicas que se utilizem de dados pessoais, responsabilizando aqueles que não respeitarem as diretrizes ditadas na lei. As sanções administrativas estão previstas e regulamentadas nos arts. 52, 53 e 54 da lei, indo desde advertências que exigem adoção de medidas corretivas até eliminação de empresas no meio virtual.

Em virtude dos fatos mencionados, empresas e o próprio governo não estão preparados para tal mudança legislativa, visto que muitos dados já podem estar espalhados e em poder de vários parceiros ou até mesmo já estarem sendo usados com finalidades maliciosas.

CONSIDERAÇÕES FINAIS

No presente trabalho buscou-se a demonstração da evolução dos meios tecnológicos e aparelhos em rede, com a consequente aparição e elevação dos crimes cibernéticos. Ainda, objetivou-se trazer a problemática do aparecimento de novas figurações de crimes convencionais cometidos por meio virtual ou mediante auxílio de recursos tecnológicos.

A tecnologia é uma ferramenta com grandes benefícios para a população, realizando atividades diversas. Porém, também, se tornou um ambiente hostil e cheio de ameaça à espreita devido à facilidade que os cibercriminosos encontraram para suas novas atuações maliciosas.

Assim como os delitos convencionais, os crimes cometidos no âmbito virtual são classificados por sua natureza. Sendo próprios aqueles cometidos por meio do computador ou qualquer outro aparelho eletrônico que atinge o bem jurídico no meio virtual e os impróprios que são aqueles que mesmo sendo cometidos por aparelhos eletrônicos atingem bens fora do âmbito virtual.Há também a classificação dos cibercriminosos, podendo ser aqueles com grandes conhecimentos tecnológicos ou civis comuns com conhecimentos técnicos básicos.

A tendência é o cibercriminoso se especializar cada vez mais e com isso novas e ampliadas atuações para obtenção de resultados cada vez mais rápidos e com resultados mais danosos às vítimas. É necessário entender a dinâmica dos cibercriminosos, as formas em que o crime tradicional está migrando para o meio virtual.

Devido à sensação de impunidade e facilidade de obtenção de resultados, os cibercriminosos atuam com mais facilidade e se aproveitam, muitas vezes, da falta de conhecimento dos usuários.

Tendo em vista que o arcabouço legislativo não está conseguindo acompanhar toda a evolução tecnológica e criminosa, além da dificuldade, na fase investigativa, da polícia tentar localizar o infrator, surge a sensação de impunidade e muitas vezes os cibercriminosos não são punidos adequadamente e na mesma proporção da dano causado à vítima.

Portanto, pode-se afirmar que os cibercrimes necessitam de um aparato legislativo específico, conforme a Convenção de Budapeste já havia recomendado, havendo punições mais severas e, consequentemente, o receio para cometimento de delitos. Ou seja, deve-se ter uma estrutura de controle e repressão estatal qualificada, além do apoio moral e psicológico à vítima.

REFERÊNCIAS

ALVES, Matheus de Araújo. **Crimes digitais:** análise da criminalidade digital sob a perspectiva do Direito Processual Penal e o Instituto da Prova. 1. ed. Belo Horizonte: Dialética, 2020.

BARRETO, Alesandro Gonçalves; KUFA, Karina; SILVA, Marcelo Mesquita. **Cibercrimes e seus reflexos no Direito brasileiro.** 2. ed. São Paulo: Juspodivm, 2021.

BRASIL. **Constituição Federal da República Federativa do Brasil de 1988.** Promulgada em 05 de outubro de 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 30 mar. 2022.

BRASIL. **Decreto-Lei nº 2.848, de 07 de dezembro de 1940: Código Penal.** 1940. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848.htm. Acesso em: 30 mar 2022.

BRASIL. **Lei 12.735, de 30 de novembro de 2012.** 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12735.htm. Acesso em: 31 mar 2022.

BRASIL. **Lei 12.737, de 30 de novembro de 2012.** 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 31 mar 2022.

BRASIL. **Lei 12.965, de 23 de abril de 2014.** 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 04 abr 2022.

BRASIL. **Lei 14.155, de 27 de maio de 2021.** 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14155.htm#art1. Acesso em: 31 mar. 2022.

CRESPO, Marcelo Xavier de Freitas. **Crimes digitas: do que estamos falando?** 2015. Disponível em : https://canalcienciascriminais.jusbrasil.com.br/noticias/199340959/crimes-digitais-do-que-estamos-falando#:~:text=São%20todas%20as%20condutas%20previstas,ser%20praticado%20de%20outra%20forma. Acesso em: 29 mar. 2022.

DESLANDES, Maria S.S.; ARANTES, Álisson R.. **Os perigos dos crimes virtuais nas redes sociais,** 2017. Disponível em: https://periodicos.pucminas.br/index.php/sinapsemultipla/article/view/16488/12745. Acesso em: 25 mar. 2022.

SENNA, Felipe; FERRARI, Daniella. **Convenção de Budapeste e crimes cibernéticos no Brasil.** 2020. Disponível em: https://www.migalhas.com.br/depeso/335230/convencao-de-budapeste-e-crimes-cibernetics-no-brasil. Acesso em: 04 abr 2022.

SANTIN, Altair Olivio. **Os desafios e impactos da lei geral de proteção de dados.** 2019. Disponível em: https://www.migalhas.com.br/depeso/312847/os-desafios-e-impactos-da-lei-geral-de-protecao-de-dados. Acesso em: 04 abr 2022.

SIGNIFICADO DE *MODUS OPERANDI*. Significados. Disponível em: https://www.significados.com.br/modus-operandi/#:~:text=Modus%20operandi%20%C3%A9%20uma%20express%C3%A3o,literal%20para%20a%20l%C3%ADngua%20portuguesa. Acesso em: 30 mar. 2022

SYDOW, Spencer Toth. **Crimes informáticos e suas vítimas.** 2. ed. São Paulo: Saraiva, 2015.

VIANNA, Túlio Lima. **Do acesso não autorizado a sistemas computacionais: fundamentos de Direito Penal informático.** Disponível em: https://www.bibliotecavirtual.ufmg.br/dspace/bistream/handle/1843/BUOS-96MPWG/disserta_o_t_lio_lima_vianna.pdf?sequence=1. Acesso em: 30 mar. 2022.

ZANIOLO, Pedro Augusto. **Crimes modernos: o impacto da tecnologia no direito.** 4. ed. Salvador: Juspodivm, 2021.