ARTIGO

É POSSÍVEL A PREVENÇÃO E COMBATE AOS TEMIDOS CRIMES VIRTUAIS?

Luiza Ananda Queiroz de Souza
Yasmin Cervinski

Resumo

O presente artigo tem por finalidade aprofundar a análise sobre os crimes cibernéticos ou cybercrimes e como eles surgiram, relacionando o surgimento deles com a evolução do computador e da Internet, visando uma possível solução para o combate e prevenção dos mesmos. Nesse artigo buscou-se identificar as principais modalidades dos crimes virtuais, bem como apresentar alguns avanços legislativos quanto à tipificação deles, assim como suas respectivas punibilidades. No decorrer do artigo será analisado que no Brasil não há legislação suficientes para a punição desses crimes no âmbito virtual, devido a isso, os crimes cibernéticos no Brasil crescem cada vez mais, levando os crackers e pessoas comuns à praticarem condutas ilícitas por meio da Internet, propiciando dano a outrem, como por exemplo os crimes contra honra, pedofilia, estelionato virtual e entre outras condutas que serão analisadas no presente artigo.

PALAVRAS-CHAVE: Âmbito Virtual, Combate, Crimes Cibernéticos, Internet, Legislação.

1 INTRODUÇÃO

No mundo contemporâneo, a Internet passou a fazer parte do cotidiano de praticamente todos os cidadãos, isso abrange desde os bebês até os idosos. O surgimento dela se deu para um meio puramente militar, onde era preciso o compartilhamento de dados entre lugares distantes, tudo isso no bojo da Guerra Fria. Ao final da guerra, muitas universidades começaram a se utilizar desse meio como um novo meio de comunicação e, o que era utilizado como um instrumento militar, tornou-se parte do cotidiano de todos os seres

humanos, o que, claramente, trouxe inúmeros benefícios e facilidades. Com tamanha facilidade de acesso, os usuários navegam por diversos sites, interagem com outros usuários, o que possibilita uma gama de atividades, sendo profissionais, pessoais, de entretenimento etc., porém, como tudo tem seu malefício, com a Internet não seria diferente.

Com o crescimento e avanço da Internet, abriu-se uma margem para o cometimento de crimes, esses chamados de crimes virtuais e seus sinônimos, sendo eles: "crimes cibernéticos", "crimes informáticos", "delito informático", "cybercrimes". Com o mundo cada vez mais conectado, os crimes virtuais estão em pauta na sociedade atual. A internet tornou-se essencial para a população que proporciona autonomia para as pessoas. Porém, alguns indivíduos não sabem se utilizar dessa autonomia corretamente, cometendo atos ilícitos por meio da Internet e, esses atos estão crescendo rapidamente e estão ocorrendo com muita frequência.

Logo, é necessário analisar: é possível a prevenção e o combate acerca dos temidos crimes virtuais? A problemática manifesta a indagação sobre o que versa o crime cibernético e qual é a forma eficiente de combater esse crime, que, em diversos momentos, o sistema penal não foi capaz de suprir, resultando em impunidade.

Por fim, para alcançar tal propósito, no presente artigo foi realizado um estudo aprofundado e análise dos principais meios de comunicação, sendo eles o computador e a Internet, abordando os conceitos de crimes virtuais; ciberespaço; além de analisar modalidades de crimes cometidos no meio virtual, legislações pertinentes sobre o tema e possíveis soluções e prevenções, tendo como coleta para esse conhecimento adquirido alguns artigos jurídicos específicos, bem como materiais disponibilizados por meio eletrônico, como legislação e sites oficiais.

2 **DESENVOLVIMENTO**

2.1 EVOLUÇÃO HISTÓRICA

O ser humano, desde seus primórdios, vem buscando formas para facilitar a convivência em sociedade. Durante todo século XX, o mundo

presenciou diversas evoluções tecnológicas, dentre elas: o computador e a Internet. O primeiro, com sua evolução no decorrer dos anos, aperfeiçoou as formas de comunicação entre os povos, característica essencial para uma boa vivência em sociedade, o qual teve início em 1943; e, a Internet tendo seu desenvolvimento em 1969, iniciando no contexto da Guerra Fria (FROTA, 2017; PAIVA, 2017).

2.1.1 Surgimento e funções do computador e da Internet

O computador, juntamente com a internet, mudou totalmente o cotidiano de todos os seres humanos. O mundo teve e tem em suas mãos uma das criações mais grandiosas realizadas pelo homem. Os computadores são aparelhos eletrônicos que recebem, armazenam e produzem informações de modo automático, fazendo parte do nosso cotidiano, aumentando cada vez mais seu número de usuários pelo mundo. O termo "computador" vem do verbo "computar", que significa "calcular". O computador que conhecemos hoje passou por longas transformações, acompanhando o avanço de áreas como a da matemática, engenharia, eletrônica e, também, da sociedade durante os séculos XX e XXI, porém, vale ressaltar que seu início ocorreu apenas na modernidade. A evolução deste está dividido em quatro gerações/períodos (SILVA, 2019).

Os computadores da primeira geração (1951 – 1959) funcionavam por meio de circuitos e válvulas eletrônicas, estes sendo imensos e pesados, podendo citar como exemplo o Eletronic Numerical Integrator and Computer (ENIAC) em português Computador Integrador Numérico Eletrônico, desenvolvido em 1946, utilizado com finalidade militar. Já a segunda geração (1959 – 1965) se utilizava de transistores para o funcionamento dos computadores, considerado um avanço para a época, bem como começaram a ser usados comercialmente. Na terceira geração (1965 – 1975), os computadores deixaram de lado os transistores e passaram a utilizar os circuitos integrados, momento em que começou a utilização dos computadores para uso pessoal, pelo fato de terem diminuído de tamanho e obterem uma maior capacidade de processamento. Por fim, a quarta e

última geração (1975 – até os dias atuais), com o desenvolvimento da tecnologia da informação, os computadores aumentaram a velocidade de processamento, diminuindo ainda mais seu tamanho, expandindo, assim, cada vez mais o uso pessoal de computadores (SILVA, 2019).

Em relação à Internet, ela teve sua origem durante a Guerra Fria, em meados dos anos 60. Na década de 1980 foi criado o termo "Internet", sendo ampliado comercialmente, e, em 1990, a Internet alcançou seu auge, atingindo todos os meios de comunicação. No Brasil, a Internet surgiu no final da década de 80, momento em que universidades brasileiras compartilhavam informações com os Estados Unidos. Em 1989, foi fundada a Rede Nacional de Ensino e Pesquisa (RNP), dando força à divulgação e acesso, com a finalidade de expandi-la pelo Brasil (COLLI, 2021).

Segundo INELLAS (2009), a internet é uma rede de computadores, ligadas por redes menores, comunicando-se entre si através de um endereço de IP. Nesse endereço de IP, todas as informações possíveis são trocadas, em um curto espaço de tempo, o que se torna um problema devido à grande quantidade exposição que há. Por esse fato, o cometimento de condutas ilícitas nesse meio torna-se possível, surgindo, assim, os crimes cibernéticos.

É evidente que todas revoluções e avanços trazem consigo algumas desvantagens, e com a Internet não seria diferente. Mesmo diante de todas as vantagens, como por exemplo a utilização da mesma para estudos à distância, o que foi muito usado nos últimos tempos em decorrência da pandemia mundial do Covid-19; conhecer novas culturas e costumes acerca do mundo; comunicação global; lazer; novas profissões, usando como exemplo o e-commerce; distribuição de informação instantânea etc., esse meio apresenta inúmeras desvantagens, devido à rapidez de seus meios de comunicação que, infelizmente, possibilitou os temidos e conhecidos crimes cibernéticos, considerado uma ameaça global.

2.2 CIBERESPAÇO:

Conceituar o ciberespaço é um tanto quanto delicado, pois este constitui um espaço geográfico ilimitado. Ciberespaço é um produto da

matriz cibernética, está intimamente ligado, dentro da cultura cibernética, com o desenvolvimento do cyberpunk, em meados dos anos 80. Após a Segunda Guerra Mundial, a influência desta possibilitou o desenvolvimento e o emergir de uma cultura na qual a tecnologia tornara-se parte de seu cotidiano (COLLI, 2021).

2.3 CRIMES CIBERNÉTICOS:

O histórico dos crimes cibernéticos remete-se à década de 1970, quando, pela primeira vez, foi definido o termo "hacker". Este sendo descrito como programadores que possuem grande conhecimento das áreas tecnológicas, no geral, não possuindo intenções criminosas, mas, devido ao seu amplo conhecimento, nada impede que os mesmos pratiquem o crime, por isso, aos olhos de muitos, esse conceito está relacionado aos crimes virtuais. Porém, os verdadeiros criminosos são os "crackers" que, segundo Cassanti (2014, p. 97), praticam a quebra de sistemas de segurança, códigos de criptografia e senhas de acesso a redes, ilegalmente, para fins criminosos.

Com o avanço das tecnologias, foi, cada vez mais, abrindo espaço para crimes cibernéticos e seus sinônimos, quais sejam: "cibercrimes"; "crimes digitais"; "crimes eletrônicos"; "crimes informáticos"; que consistem em condutas criminosas realizadas por meios eletrônicos (computadores, celular e/ou Internet) que podem atingir pessoas físicas como, também, um sistema inteiro, podendo causar danos e prejuízos incalculáveis (FROTA, 2017; PAIVA, 2017).

O cibercrime (traduzindo o termo do inglês cybercrime, termo originado na França, na cidade de Lyon) se divide em crimes puros ou próprios, aqueles praticados necessariamente por computador e realizam-se e consomem-se em meio eletrônico, no qual a informática é o objeto jurídico tutelado, tendo como exemplo a invasão de dados armazenados; e, impuros ou impróprios, aqueles em que o agente se vale do computador para produzir um resultado naturalístico, que ofenda o mundo físico ou espaço real ameaçando ou lesando bens diversos da informática (SILVEIRA, 2015).

Com a evolução tecnológica e nos sistemas de dados, é evidente que muitos cidadãos recorram dessa ferramenta para guardar seus dados, como memórias em formato de fotos; estudos; arquivos pessoais e profissionais. Diante disso, torna-se extremamente importante que haja uma legislação a fim de proteger esses registros e assegurar a visibilidade de tais apenas pelos seus proprietários e que haja, também, punições aos invasores e seus crimes ocorridos na esfera virtual (MEDEIROS, 2020).

Tal segurança é prevista constitucionalmente, em seu artigo 5º (quinto), que diz que "Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade", nos termos de seu inciso X, qual seja: "X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação" (BRASIL, 1988).

2.4 ESPÉCIES DE CRIMES VIRTUAIS

Os crimes virtuais são aqueles cometidos via internet e podem ser enquadrados no Código Penal, onde haverá as respectivas punições de acordo com cada caso, tendo seu sujeito ativo como qualquer pessoa que usa desse meio virtual para o cometimento do ato ilícito e, o sujeito passivo será qualquer pessoa, física ou jurídica, que são usuários e navegam na Internet. Existem diversos crimes existentes na esfera virtual, sendo alguns deles: estelionato virtual, crimes contra a honra, cyberbullying, invasão de privacidade etc.

O Código Penal, em seu art. 171, caput, dispõe que praticam o crime de estelionato quem "Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento" (BRASIL, 1940).

O crime de invasão de privacidade trata-se do acesso sem autorização, não necessariamente com a violação de medidas de segurança. No Brasil, há a Lei 12.737/2012 que prevê as respectivas punições a esses crimes. O que se

procura é resguardar o cidadão com relação aos seus dados que estão disponibilizados em redes, pois os dados pessoais não podem ser tratados como mercadoria (SILVA, 2019).

Os crimes contra a honra estão previstos nos artigos 138, 139 e 140 do Código Penal. A divulgação de informações inverídicas, constitui crimes contra a honra. A honra são as qualidades físicas, morais e intelectuais de um indivíduo, devendo ser respeitada no meio social onde se convive, também, considerado um patrimônio que a pessoa possui, sendo que deve ser protegido. A honra é uma garantia constitucional, previsto no artigo quinto, em seu inciso X. Existem três tipos de crimes contra a honra, sendo eles: calúnia, difamação e injúria (SILVA, 2019).

O crime de Calúnia é definido no art. 138 do Código Penal, que prevê "caluniar alguém, imputando-lhe falsamente fato é definido como crime" (BRASIL, 1940). Neste crime a honra objetiva da vítima é abalada, isto é, o agente atribui a vítima a prática de fato definido como crime, tendo ciência que a imputação é falsa, abalando sua reputação perante a sociedade (SILVA, 2019).

O crime de Difamação é definido no artigo 139 do Código Penal Brasileiro, prevendo em sua redação: "difamar alguém, lhe imputando fato ofensivo à sua reputação" (BRASIL, 1940). Esse crime afeta a honra objetiva da vítima, onde se preocupa com o que terceiros irão pensar sobre sua pessoa. Esse crime é praticado na internet em diferentes formas, seja por e-mails enviados a vítima ou outras pessoas contendo algum fato que ofenda sua honra objetiva, ou quando publique em redes sociais as mesmas ofensas (SILVA, 2019).

O crime de Injúria é definido no art. 140 do Código Penal: "Injuriar alguém, ofendendo a dignidade ou o decoro" (BRASIL, 1940). Este crime consiste na exposição de qualidade negativa da vítima por um terceiro, que diga respeito aos seus atributos morais, intelectuais ou físicos, afetando de forma significativa a honra subjetiva da vítima (SILVA, 2019).

E, por fim, o Cyberbullying é uma intimidação feita através da Internet, sendo uma extensão do bullying escolar, no qual o veículo mais utilizado para

a prática desse crime são as redes sociais, podendo acometer tanto crianças e adolescentes como adultos (CARVALHO, 2018).

2.5 ORDENAMENTO JURÍDICO PÁTRIO ACERCA DOS CRIMES VIRTUAIS

Nas últimas décadas a preocupação devido a popularização da internet no mundo todo vem aumentando cada vez mais. Com o avanço da tecnologia, democratização e o fácil acesso as redes sociais, o sistema judiciário brasileiro sentiu a necessidade de tipificar ainda mais rigorosamente os crimes cometidos em ambiente virtual (SILVA, 2019).

2.5.1 Invasão de privacidade - Lei N° 12.737/2012

Em relação aos crimes de invasão de privacidade, vemos uma evolução legislativa chamada de Lei nº. 12.737/2012, popularmente conhecida como Lei Carolina Dieckmann. Essa Lei é uma alteração no Código Penal Brasileiro voltado para crimes informáticos. Antigamente, não se tinha uma tipificação para crimes desse meio virtual, porém, essa lacuna foi preenchida (COLLI, 2021, p. 82),

Após o ano de 2012, essa nova legislação entrou em vigor, passando a tipificar o crime previsto no Código Penal brasileiro, no seu artigo 154-A, prevendo em sua redação que "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" (BRASI, 1940)

2.5.2 Marco Civil da Internet

Em 2014, no Congresso Nacional, foi aprovada a Lei 12.965/14 – o Marco Civil da Internet, o MCI que ficou conhecido como a Constituição da Internet Brasileira. Essa Lei, inicialmente, apresenta de maneira sistematizada dez princípios elaborados pelo Comitê Gestor da Internet Brasileira, sendo eles: Liberdade, Privacidade e Direitos Humanos; Governança Democrática e Colaborativa; Universalidade; Diversidade; Inovação; Neutralidade da Rede;

Inimputabilidade da Rede; Funcionabilidade, Segurança e Estabilidade; Padronização e Interoperabilidade; e, Ambiente Legal e Regulatório (NASCIMENTO, 2019).

Essa Lei foi criada com muitos objetivos, sendo: definir os direitos oriundos da utilização da internet, prevendo o que pode ou não fazer no âmbito civil antes de criminalizar condutas praticadas na internet. O MCI é considerado um novo conjunto de padrões para o Brasil e para o restante do mundo. Seus dez princípios representam um alicerce responsável por garantir a liberdade de expressão, a privacidade e os direitos humanos no âmbito digital, mas sem impedir o controle necessário a segurança de dados, sistemas pessoais e de empresas na rede mundial de computadores (NASCIMENTO, 2019).

2.6 COMBATE AOS CRIMES VIRTUAIS:

A criminalidade virtual é um perigo global. A prática dos mesmos torna-se mais frequente a cada dia. Com o isolamento social, em decorrência da pandemia do Covid-19, esses delitos aumentaram abundantemente no ano de 2020 e, no Brasil, estima-se que por minuto ocorrem cerca 23 condutas criminosas pelo meio virtual (GLOBO, 2020).

De acordo com os peritos criminais dos Institutos de Criminalística do Brasil, algumas ações para o combate e prevenção desses crimes são a implantação de tecnologias de segurança da informação; a aquisição ou desenvolvimento de ferramentas com tecnologia forense em computadores para executar exames periciais; monitoramento mediante mandado judicial em redes com suspeitas de práticas fraudulentas; e, direcionamento, estratégia e união de instituições nacionais e internacionais.

Ademais, algumas dicas a serem seguidas, ainda de acordo com esses peritos criminais, são o investimento em segurança da informação, utilizada para proteção dos dados, arquivos, informações que estão em algum dispositivo ou até mesmo na nuvem. Deve-se conscientizar sobre a importância do acesso seguro à Internet, tanto à pessoas físicas quanto pessoas jurídicas; a criação de senhas seguras, devendo sempre optar por senhas complexas abrangendo números, letras e caracteres especiais, além

de não usar a mesa senha para diversas contas virtuais; a ampliação do cuidado ao abrir e-mails e sites desconhecidos; realização de backup periodicamente; executar atualizações de segurança para evitar a vulnerabilidade e se proteger de ameaças; a instalação de um antivírus de confiança, para bloquear ameaças e eliminar vírus, ativando o firewall para impedir a invasão de códigos maliciosos; e, por fim, monitore e tenha senso crítico de uso em relação às promoções, sorteios, descontos e outras ações que podem ser fraudulentas, evitando sempre cadastrar dados pessoais e bancários em sites não confiáveis, ou mandá-los por e-mail.

Devido ao número excessivo de crimes virtuais, há uma carência de profissionais especializados nessa área. Para combater esses crimes, torna-se necessário que o perito digital tenha formação superior na área de computação, tecnologia da informação ou áreas afins, bem como atualização no conhecimento por meio de treinamentos na área computacional forense para acompanhar novas tecnologias que surgem com o passar do tempo, investigar o crime digital e, principalmente, identificar o cracker (FROTA, 2017; PAIVA, 2017).

O cidadão que for vítima de um delito virtual deverá notificar o provedor encarregado pelo site ou rede social em que ocorreu a infração penal relatando o ocorrido. A empresa, ao ser notificada, tem obrigação de retirar a página do ar onde ocorreu o delito e identificar o endereço de IP do computador agressor (CAMPANHOLA, 2018).

Contudo, qualquer vítima terá o direito de reparação ao dano causado à sua imagem e de buscar responsabilização do agente ativo, inclusive para evitar que o mesmo persista na conduta ilícita. Portanto, o indivíduo que tem sua imagem desonrada no meio virtual, tem autonomia e está amparado pela Lei. Tal previsão está no próprio Código Penal ou, de acordo com o dano sofrido pela vítima, caberá indenização por danos morais, previsto no Código Civil Brasileiro, no seu artigo 186, que prevê que "aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito" (BRASIL, 2002).

2.7 DIFICULDADE NO COMBATE:

O uso de aparelhos eletrônicos, juntamente com a Internet, demonstra o avanço desses meios para a sociedade. Diante de todos os benefícios que eles trazem aos humanos, infelizmente, torna-se acessível as condutas criminosas nesse meio, pois os usuários ficam vulneráveis aos infratores. De fato, há poucos combatentes contra os crimes virtuais (TERRA, 2019), por isso, os agressores aproveitam para invadir sistemas e praticar o roubo de dados.

É de extrema dificuldade punir crimes dessa espécie, pois, geralmente, os criminosos agem sem deixar suspeitas, associado ao mundo tecnológico que os permitem agir de forma anônima e silenciosa. Ademais, os criminosos agem por meio do uso de dados falsos, proliferação de vírus e o uso da internet em locais públicos, visto que estes disponibilizam fácil acesso.

Por outro lado, segundo Vagner Nunes (TERRA, 2019) os profissionais competentes dessa área são escassos, isso ocorre pelo fato de os crimes e ameaças nesse setor crescerem e evoluírem rapidamente no decorrer dos anos, bem como a falta de capacitação desses profissionais. Devido a isso, é de extrema importância que surjam mais profissionais especializados nessa área, para conseguir acompanhar o rápido desenvolvimento desses crimes, e, também, que seja disponibilizado a esses combatentes todos os meios disponíveis e eficazes para um melhor desempenho de seu trabalho.

No entanto, no Brasil, uma das dificuldades principais é a falta de obtenção de provas e as devidas punições dos delitos praticados. Além disso, a falta de profissionais capacitados nesse ramo para o combate aos crimes virtuais é outra dificuldade enfrentada no país, em razão disso é necessário que esses profissionais, bem como os órgãos destinados a esse combate, se atualizem para realizar seu trabalho de forma desejável. Outra dificuldade enfrentada pelo Brasil é o atraso na criação de leis que evoluam juntamente com a sociedade. São dificuldades como essas que possibilitam o aumento significativo desses crimes.

De acordo com um relatório divulgado por uma empresa de segurança cibernética chamada Symantec, juntamente com a Organização dos Estados Americanos (OEA), no ano de 2014, o Brasil está situado em primeiro lugar no

ranking latino-americano de atividade maliciosa gerado por país, alcançando a marca de mais de R$ 18 bilhões em prejuízos causados pelo crime virtual.

3 **CONCLUSÃO**

Diante do exposto, no presente artigo buscou-se apresentar a evolução histórica dos meios tecnológicos, abordando sobre o computador e Internet e suas funções, bem como demonstrar de que forma essas tecnologias contribuíram para o surgimento e crescimento desenfreado dos temidos crimes cibernéticos, que são uma ameaça global e podem acometer a qualquer cidadão; e, também, as possíveis formas de combate e sua dificuldade, visto que no Brasil ainda há uma escassez de leis e profissionais capacitados para isso.

Em relação à dificuldade no combate aos crimes virtuais, mesmo com alguns avanços, citando como exemplo as Leis Carolina Dieckmann e Marco Civil, esses delitos continuam ocorrendo em grande quantidade. Em vista disso, é evidente que os avanços ocorridos até os dias atuais acerca dos meios de combate ainda são escassos comparados ao grande mundo cibernético e a infindável prática de atos ilícitos por parte dos agressores.

Diante disso, torna-se necessário que os operadores do direito e autoridades competentes, pensem em alguma forma de conter esses crimes de uma forma eficaz, para que, assim, os cidadãos possam navegar livremente e com segurança pelas redes na Internet. Para tal fim, é importante que seja aperfeiçoado as práticas de combate aos crimes virtuais; que aos profissionais dessa área seja disponibilizado um desenvolvimento especializado para alcançar a evolução desses crimes, capacitação na área informática, investimentos em tecnologias para aumentar a busca de delitos, treinamento policial, criação de delegacias com profissionais especializados na área virtual; e a criação de novas leis que acompanhem a evolução desses crimes, porém, a criação de uma nova norma penal incriminadora só

tem seu efeito esperado na sociedade quando as autoridades competentes são qualificadas para isso.

Além disso, o cidadão que tiver seu direito lesado tem direito à reparação. Ademais, algumas formas para se prevenir contra esses delitos são a implantação de tecnologia de segurança da informação; monitorar ações suspeitas e sempre denunciá-las; investimentos para a proteção e segurança dos dados, informações pessoais e arquivos; e, cabe ao Estado conscientizar os cidadãos sobre a gravidade desses crimes.

Após um estudo aprofundado sobre o tema, conclui-se que é de extrema importância que haja a imediata tipificação no ordenamento jurídico brasileiro de condutas criminosas por meio da Internet para a proteção dos usuários e para reprimir os agressores.

REFERÊNCIAS

BRASIL. Código Civil. (2002). Disponível em: http://www.planalto.gov.br/ccivil_03/leis/2002/l10406.htm. Acesso em: 18 abr. 2021.

BRASIL. Lei nº 2848, de 7 de dezembro de 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 18 abr. 2021.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm>. Acesso em: 21 abr. 2021

CAMPANHOLA, Nadine Finoti. Crimes Virtuais Contra a Honra. 2018. Disponível em: http://www.conteudojuridico.com.br/consulta/Artigos/51558/crimes-virtuais-contra-a-honra#:~:text=Os%20crimes%20cibern%C3%A9ticos%20ou%20virtuais,uma%20a%C3%A7%C3%A3o%20contra%20o%20ofensor. Acesso em: 17 abr. 2021.

CARVALHO, Gabriel Chiovetto. Crimes Cibernéticos. 2018. Disponível em: https://conteudojuridico.com.br/consulta/Artigos/51878/crimes-ciberneticos. Acesso em: 18 abr. 2021.

CASSANTI, Moisés de Oliveira. Crimes virtuais, vítimas reais. 1. ed. Rio de Janeiro: Brasport, 2014.

DATA CENTER DYNAMICS. OEA e Symantec apresentam relatório sobre cibersegurança na América Latina. 2014. Disponível em: https://www.datacenterdynamics.com/br/not%C3%ADcias/oea-e-symantec-apresentam-relat%C3%B3rio-sobre-ciberseguran%C3%A7a-na-am%C3%A9rica-latina/ . Acesso em: 19 abr. 2021

COLLI, Maciel. Limites e perspectivas para a investigação de Crimes Cibernéticos. 2. ed. Curitiba: Jurua, 2021.

FROTA, Jéssica Olivia Dias; PAIVA, Maria de Fátima Sampaio. CRIMES VIRTUAIS E AS DIFICULDADES PARA COMBATÊ-LOS. 2017. Disponível em: https://flucianofeijao.com.br/novo/wp-content/uploads/2019/11/CRIMES_VIRTUAIS_E_AS_DIFICULDADES_PARA_COMBATELOS.pdf. Acesso em: 21 abr. 2021.

INELLAS, Gabriel Cesar Zaccaria. Crimes na internet. 2. ed., atual. e ampl. São Paulo: Juarez de Oliveira, 2009. p. 5. Acesso em: 19 abr 2021

GLOBO. Crimes virtuais crescem durante o isolamento social. 2020. Disponível em: https://g1.globo.com/jornal-nacional/noticia/2020/07/10/crimes-virtuais-crescem-durante-o-isolamento-social.ghtml. Acesso em: 17 abr. 2021.
INELLAS, Gabriel Cesar Zaccaria. Crimes na internet. 2. ed., atual. e ampl. São Paulo: Juarez de Oliveira, 2009.

KASPERSKY. Dicas de como se proteger contra crimes cibernéticos. Disponível em: https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime. Acesso em: 17 abr. 2021.

MEDEIROS, Gutembergue Silva. Crimes Cibernéticos: Considerações Sobre a Criminalidade na Internet. 2020. Disponível em: https://ambitojuridico.com.br/cadernos/direito-penal/crimes-ciberneticos-consideracoes-sobre-a-criminalidade-na-internet/#_ftn1. Acesso em: 16 abr. 2021.

NASCIMENTO, Samir de Paula. Cibercrime: Conceitos, modalidades e aspectos jurídicos-penais. 2019. Disponível em: https://ambitojuridico.com.br/cadernos/internet-e-informatica/cibercrime-conceitos-modalidades-e-aspectos-juridicos-penais/. Acesso em: 14 abr. 2021.

SILVA, Ellen Barros. Crimes cibernéticos: é possível combater esses crimes virtuais aplicando ao caso concreto a legislação pertinente? 2019. Disponível em: https://jus.com.br/artigos/77977/crimes-ciberneticos-e-possivel-combater-esses-crimes-virtuais-aplicando-ao-caso-concreto-a-legislacao-pertinente. Acesso em: 20 abr. 2021.

SILVEIRA, Artur Barbosa da. Os crimes cibernéticos e a Lei nº 12.737/2012. 2015. Disponível em: https://conteudojuridico.com.br/consulta/Artigos/43117/os-crimes-ciberneticos-e-a-lei-no-12-737-2012. Acesso em: 18 abr. 2021.

TERRA. Carência de profissionais em cyber segurança facilita crimes na internet. 2019. Disponível em: https://www.terra.com.br/noticias/dino/carencia-de-profissionais-em-cyber-seguranca-facilita-crimes-na-internet,b76978ec3e1077ca0b000ab9094abfa5qmm40vsm.html. Acesso em: 21 abr. 2021.

Sobre o(s) autor(es)
Luiza Ananda Queiroz de Souza. Formanda em direito pela Universidade do Oeste de Santa Catarina - UNOESC, campus São Miguel do Oeste. Email: luizaananda.souza@gmail.com
Yasmin Cervinski. Formanda em direito pela Universidade do Oeste de Santa Catarina - UNOESC, campus São Miguel do Oeste. Email: yascervinski_@hotmail.com