OS SUJEITOS ATIVOS NO CIBERCRIME E A RESPONSABILIDADE PENAL DO OFENSOR

Jéssica Rafaela Nunes Sobrinho[1]
Sergio Grott[2]

RESUMO

O presente artigo busca identificar quem são os sujeitos ativos do cibercrime, dada a enorme importância do meio tecnológico, bem como analisar a responsabilidade penal dos sujeitos que cometem esses delitos. Para alcançar tais objetivos, pretende-se analisar o contexto histórico desde o advento da internet, o surgimento do cibercrime e seu conceito, para classificá-los de acordo com as terminologias empregadas no ambiente virtual e legislações já criadas que abrangem esta temática, considerando que esta matéria não pode ser estática, devendo proceder-se a uma adaptação do direito penal à realidade informática. Para isso, este artigo possui abordagem qualitativa, voltada para o estudo bibligráfico, demonstrando-se como uma prática comum de crimes, que demandam de adaptações legislativas para que consigam acompanhar a volatilidade dos meios informáticos e garantir segurança a todos que utilizam.

Palavras-chave: Cibercrime. Sujeito Ativo. Responsabilidade Penal.

ABSTRACT

This article seeks to identify who are the active subjects of cybercrime, given the enormous importance of the technological environment, as well as to analyze the criminal responsibility of subjects who commit these crimes. To achieve these goals, it is intended to analyze the historical context since the advent of the internet, the emergence of cybercrime and its concept, to classify them according to the terminologies used in the virtual environment and legislation already created covering this theme, considering that this matter cannot be static, and criminal law must be adapted to the reality of information technology. For this, this article has a qualitative approach, focused on bibliographic study, demonstrating itself as a common practice of crimes, which require legislative adaptations so that they can keep up with the volatility of information technology and guarantee security for all who use it.

Keywords: Cybercrime. Active Subject. Criminal Liability.

[1] Graduando em Direito pelo Centro de Ensino Superior do Amapá – CEAP. Email: jessica.rafaela.nunes@gmail.com
[2] Docente do Curso de Direito do Centro de Ensino Superior do Amapá. Especialista em Direito Constitucional pela Faculdade Damásio Educacional. Graduado em Direito pela Universidade Federal do Amapá-UNIFAP. Mestre em Direito pela Uniceub. Email: sergio.grott@ceap.br

1 INTRODUÇÃO

O presente trabalho de pesquisa surgiu da necessidade de identificar quem são os sujeitos ativos dos crimes cibernéticos, suas características e os aspectos jurídicos que penalizam quem pratica esses delitos. Assim, surgiu o tema deste estudo, qual seja os sujeitos ativos no cibercrime e a responsabilidade penal do ofensor. A pesquisa do tema justificou-se pela extrema importância de estudar a evolução do cometimento de delitos por intermédio do meio tecnológico que apenas tende a crescer, bem como a evolução do sistema normativo.

Considerando que se trata de atividades criminosas praticadas através de um dispositivo conectado à rede de internet, sobreveio a seguinte pergunta de pesquisa: Quem são os sujeitos ativos dos crimes cibernéticos e como o ofensor pode ser responsabilizado? Entende-se que para responder a pergunta é importante verificar que os sujeitos ativos do cibercrime não são popularmente conhecidos pela sociedade em geral, o que resulta na dificuldade em responsabilizá-los, considerando o obstáculo das investigações e do ajustamento legislativo para puni-los.

O objetivo geral deste trabalho é identificar os sujeitos ativos dos crimes cibernéticos e seus aspectos jurídicos penais no direito brasileiro. Relativamente aos objetivos específicos para o alcance da perfeita análise do crime em estudo, busca-se descrever o surgimento da internet e a origem e particularidades conceituais do cibercrime; analisar os sujeitos ativos dos crimes cibernéticos e demonstrar a responsabilidade penal diante do cometimento dos cibercrimes à luz do direito brasileiro.

Por meio dos objetivos do desenvolvimento desta pesquisa, confirma-se a relevância deste trabalho à ciência jurídica e à sociedade, pois busca-se expandir a informação a respeito do lado negativo que acomete a internet, uma vez que se trata do meio mais utilizado no mundo por toda a sociedade, sendo um instrumento utilizado no trabalho, estudo, cultura e lazer, de modo que buscamos contribuir para a comunidade científica.

Com o advento da internet, a realidade da sociedade atual pode ser definida por uma população conectada, que vive a era digital e suas facilidades. Tem-se uma evolução tecnológica e globalização avançada de forma que todos dependem e usufruem demasiadamente de dispositivos eletrônicos conectados à rede de internet. Contudo, nota-se uma preocupação acerca dos crimes que envolvem esse ambiente virtual.

O presente trabalho tem como objetivo analisar a figura do sujeito que pratica esses crimes e os aspectos penais que o envolvem na esfera virtual. Que, atualmente, se trata de uma plataforma popular, de modo que a previsão é de superação, pois o escopo é incessantemente uma conexão superior, tal como, melhor democratização da internet.

No que concerne à sociedade, busca-se expandir o conhecimento da figura de quem pratica o crime, pois este afeta diretamente a coletividade, essa é, todos os sujeitos que utilizam o meio virtual que podem se tornar sujeitos passivos do cibercrime, vítimas do lado negativo que assola o mundo tecnológico. Por isso, tem como objetivo também para a ciência jurídica, apresentar a devida relevância e difusão para que as pessoas compreendam que é possível definir quem comete esses atos e que existe amparo legal.

O presente estudo utiliza como base a pesquisa de cunho bibliográfico, através de doutrinas, artigos científicos, teses e dissertações a fim de se tomar nota das divergentes correntes de opinião sobre o assunto, cujo foco é o cibercrime e seus sujeitos ativos. A abordagem da pesquisa é qualitativa, com o aprofundamento de como será compreendido o tema tratando-se de um estudo bibliográfico, com enfoque do método hipotético-dedutivo, que se voltará para a revisão bibliográfica utilizada. Será realizada uma análise através da leitura e interpretação do material bibliográfico, tendo como base teórica a análise das teorias de Santos, Rosa, Wendt e Jorge.

2 O ADVENTO DA INTERNET E OS ASPECTOS CONCEITUAIS DO CIBERCRIME

2.1 A ORIGEM DA INTERNET

O surgimento da Internet, segundo pesquisa da rede de notícias norte-americana CNN e do Instituto de Tecnologia de Massachussets, remete-se ao período da Guerra Fria, em meados do século XX. Em que duas potências mundiais, Estados Unidos e União Soviética, disputavam uma corrida bélica, armamentista e espacial, à vista disso, surgiu a internet, por objetivos militares (JUNIOR, 2019).

No entanto, a rede ainda não possuía a denominação de internet. Essa ideia foi nomeada como ARPANET (Agência de Pesquisa Avançada e Rede, em inglês, Advanced Research Projects Agency Network) em 1969. Já a primeira conexão internacional foi realizada em 1973, até então pela ARPANET, que interligou a Inglaterra e a Noruega. (WENDT; JORGE, 2012, p.5). O título "Internet" sobreveio posteriormente, quando houve a invenção da Teia Mundial em 1986, com isso ficou mais acessível ao público, tornando esse meio de comunicação popular na década de 90 (CARNEIRO, 2012). Essa tecnologia passou a ser utilizada com outro objetivo, para estabelecer uma ligação entre as universidades americanas, e após isso, também para institutos de pesquisa de outros países.

Com a maior distribuição da internet, a pretensão era que os usuários fossem anônimos e usufruíssem de igualdade na utilização desse espaço, visando com isso garantir uma velocidade superior e eficiência, gerando assim, maior segurança nas relações interpessoais e comerciais nesse ambiente. Desse modo, o seu objetivo inicial foi afastado, houve a democratização desse meio, sendo disponível a toda a população mundial e tornando-se um espaço sem fronteiras, assim, a rede de acesso e comunicação se universalizou, contudo, tornou-se um ambiente favorável para o surgimento e propagação de ameaças.

A rede de internet possui papel essencial mundialmente, sendo hoje utilizada como uma das plataformas mais eficientes que impulsiona a economia mundial, bem como aplicada em variados setores, entre eles, econômicos, militares, de segurança, de transportes, de telecomunicações, de educação e saúde. Dando origem ao que hoje é conhecido como sociedade da informação, vez que tudo que acontece ao redor é repleto de informação.

Considerando esse contexto socioeconômico desempenhado pela internet, é possível perceber os danos que podem advir de ameaças e ataques pela rede mundial de computadores e a imensidão dos prejuízos que essa insegurança pode ocasionar. Dado que a sociedade da informação se correlaciona com a crescente dependência dos sistemas de tecnologias de informação, que são dotadas de dinamismo e volatilidade, motivo pelo qual os

cibercrimes encontram incontáveis formas de serem praticados, e assim, o tornou um evento frequente, perigoso e violador de direitos fundamentais.

Uma vez que os crimes cibernéticos deixaram de se utilizar da internet somente como objeto final do delito, para utilizar também como meio para consumação de outros crimes. Com infinitas possibilidades de aparatos para o cometimento desses crimes no meio digital, veja-se:

> Com a utilização de vírus, o criminoso conseguia obter acesso ao computador de suas vítimas. O advento da internet e a sua forma de concepção, que permite interconectar equipamentos ao arrepio da distância geográfica e do controle, aliado à facilidade de troca de informações entre usuários que nunca se viram, e provavelmente, nunca se verão, criou uma propícia para o estabelecimento de uma outra classe de programas com objetivos voltados para causar danos a terceiros. Um destes tipos de programas de computador é o chamado vírus. Vírus, então, nada mais são do que programas de computador intencionalmente desenvolvidos, em geral, com intenções maliciosas, de causar dano a um grupo específico de computadores ou à rede em geral. (SOUZA; VOLPE, 2015).

Observa-se que o advento da rede de internet, está aliado à facilidade em diferentes formas, permitindo a conexão à distância e troca de informações, porém, pode ser favorável e voltada também para o acometimento de danos a outrem, a título de exemplo referido, a utilização de programas de computador como o vírus, intencionados ardilosamente, representando a área dos crimes de natureza informática, assim dizendo, os cibercrimes.

É importante ressaltar que os Estados Unidos, país que originou a internet, foi o primeiro também em se manifestar a respeito da importância dessas ameaças tecnológicas, tipificando pela primeira vez em 1978 crimes de natureza informática. (SOUZA; VOLPE, 2015). Com o aumento dos casos desses ilícitos praticados pela internet, a importância desse novo segmento de crimes foi evidenciada. Foram realizados estudos um pouco mais aprofundados nesta área, como também, passaram a definir as pessoas que possuem demasiado conhecimento no assunto e de que forma utilizam este conhecimento.

Contudo, não se pode olvidar que esse meio de acesso propiciou de certa forma o surgimento, bem como o próprio aumento de uma série de crimes cibernéticos. E, apesar do conhecimento contemporâneo sobre essas atividades criminosas e da indispensabilidade e urgência de investida contra tais atos, é necessário categorizar, isto é, reflexionar seu ponto inicial e conceitualizar.

2.2 CONCEITO E ORIGEM DO CIBERCRIME

Com o surgimento da internet e o avanço diário da tecnologia, a população não viveu apenas dos benefícios advindos da mesma, surgindo também os crimes cibernéticos. O cibercrime demonstrou seus primeiros indícios na década de 1960, momento em que se ouviu falar e passou a ser discutido sobre os diversos crimes envolvidos com a nova tecnologia. (NASCIMENTO, 2019). Todavia, não existe consenso geral ou uma definição clara sobre o que é um cibercrime, tendo em vista que os crimes que recorrem moderadamente à tecnologia e aos aparelhos digitais são estabelecidos nesta categoria (FRANÇA; QUEVEDO, 2020).

Como ainda se discutia as abundantes denominações para a mesma modalidade do crime, inúmeros doutrinadores definiram um conceito para o Cibercrime, assim, observou-se uma subdivisão, estabelecidas como espécies de cibercrimes, aqueles praticados por meio do computador, ao mesmo tempo que outros comportam apenas aqueles que alcançam diretamente o computador.

Logo, são diversos os nomes dados para definir uma infração penal cometida através de um dispositivo ligado à rede de internet, entre eles, crime digital, crime informático-digital, crime informático, crimes cibernéticos, criminalidade informática, high technology crimes, computer related crime, dentre outros. Não há um consenso quanto à sua denominação, quanto à sua definição, quanto à tipologia e nem classificação, porém, consideramos utilizar a denominação cibercrime (SIMAS, 2014).

Diante disso, de acordo com Barbai (2013, p. 48),

> com a nomenclatura utilizada para denominar o presente trabalho, o termo cibercrime, originou-se na França, na cidade de Lyon. Durante a reunião de um subgrupo das nações do G8, que seria composto pelos países mais ricos e industrializados do mundo, que discutiu sobre os crimes praticados por dispositivos eletrônicos conectados à internet, objetivando analisar os problemas relacionados à criminalidade em razão da ampliação desta rede.

Utilizando o termo cibercrime, para Roque (2007, p. 33) é "toda conduta, definida pela lei como crime, e que o computador tiver sido utilizado como instrumento de sua perpetração". O sujeito ativo emprega, como forma de execução de sua infração, ferramentas específicas da rede de computadores, valendo-se das habilidades tecnológicas voltadas para o uso desses dipositivos, não sendo especificamente um computador, uma vez que se trata de um sentido amplo, pois a rede de computadores é um conjunto de diversos equipamentos com recursos facilitadores de comunicação.

Em sentido lato, os crimes cibernéticos englobam toda atividade criminosa através de computadores, entre outros meios de tecnologia (SILVA, 2006). Já em sentido stricto, a criminalidade de informação engloba os crimes, de acordo com Simas (2014, p. 12), "quem que o meio informático surge como parte integradora do tipo legal, ainda que o bem jurídico protegido não seja digital". Dessa forma, definiu o cibercrime como sendo as infrações penais praticadas no âmbito digital ou que estejam envolvidos com a informação digital, mediante às condutas atentatórias à direitos fundamentais, de pessoas físicas e pessoas jurídicas através dos mais diversos meios e dispositivos conectados à internet, tais como computadores, celulares e outros.

De acordo com a Comissão Europeia, inclui-se no cibercrime três tipos de atividades criminosas, os crimes tradicionais cometidos com a assistência do computador e redes de informática, os crimes relativos ao conteúdo, com a publicação de conteúdos ilícitos por meios de comunicação eletrônica, e os crimes exclusivos das redes de informação, que são cometidos exclusivamente por meio informático.

Em sua totalidade, as condutas ilícitas no meio virtual podem ser divididas em duas: ações ilícitas atípicas e crimes virtuais. Na primeira, não há previsão legal, ou seja, não sendo regida pelo código penal, podendo o causador ser responsabilizado apenas na esfera cível (WENDT; JORGE, 2012, p. 18). No segundo, esses crimes podem ser realizados de forma tradicional, isto é, por meio de computadores como é o caso dos crimes contra a honra, ou também, podem ser praticados com a utilização do computador ou alguma outra fonte com acesso à internet, por exemplo, no caso de

clonagem de cartões por meio da internet (Ibdem, p. 19).

Portanto, se trata de uma modalidade de crimes ampla, tanto como inúmeras denominações, e tal como, diversas especificidades, sejam elas, os tipos de atividades ilícitas, as divisões pelas espécies de crimes e como estão distribuídas no ordenamento jurídico brasileiro. Sabendo-se que foi em 1960 que se verificou os primeiros indícios sobre essa modalidade de crimes, repara-se que apresentava maiores incidências em casos de manipulação e sabotagem de sistemas de computadores (CARNEIRO, 2012, p. 01). Porém, foi apenas na década de 70 que os sujeitos ativos dessas infrações penais ganharam destaque e ficaram conhecidos, naquele momento, como Hackers (ANDRADE; BENTES; GUIMARÃES, 2017).

Apesar disso, ter sido denominado de forma equivocada, dado que, nesta modalidade de crime pode se analisar sua imensa abrangência. Quem praticava esses crimes tinham o conhecimento dos programadores de computador, para acessar as informações de qualquer usuário que esteja conectado na rede mundial de computadores. Ou seja, por possuírem esse determinado conhecimento informático foram reconhecidos de forma errônea, e seguem identificados de tal forma.

Já em 1980, "houve um maior crescimento de outros tipos de crimes, não apenas envolvendo vírus e softwares, como exemplo o da pirataria e pedofilia online, gerando assim, certa preocupação com a segurança virtual" (CARNEIRO, 2012, p. 01). Todavia, foram os Crackers que deram início ao uso do computador para fins ilícitos, com uma nova modalidade de crimes, começando, assim, a burlar as leis e criar novos meios de agir contra outras pessoas, com a vantagem de não serem vistos, agindo anonimamente (ANDRADE; BENTES; GUIMARÃES, 2017).

Evidencia-se, portanto, que as definições do cibercrime são extensas, bem como, sua origem foi percebida precedentemente, conquanto se trata de uma prática extremamente ampla, vez que o meio tecnológico permite infinitas possibilidades. Assim, é imperioso destacar a figura do sujeito que investe na prática do cibercrime, valendo-se dos conhecimentos tecnológicos e da desinformação dos ofendidos que são imensuráveis, tal como da sociedade em geral.

3 SUJEITOS ATIVOS DO CIBERCRIME

Entende-se por sujeito ativo o autor da infração penal, é a pessoa que, de forma direta ou indireta, pratica a conduta descrita pelo tipo penal (NUCCI, 2014). A imputação objetiva ao autor do crime, e sua comprovação é extremamente difícil frente à ausência física do sujeito ativo. Ocorre que, diante da importância da identificação do autor do crime e a dificuldade desta, surgiu a necessidade de se traçar um perfil denominando grupos que praticam determinados cibercrimes.

No que se refere ao sujeito ativo é um crime comum quanto ao agente e estes podem ter diversos níveis de gravidade, pode ser uma pessoa comum sem relevantes conhecimentos técnicos, tal como programação e internet, conquanto, pode ser uma pessoa com conhecimento técnico aprofundado. Independente ainda de sua identificação, o sujeito ativo do cibercrime é aquele que desfruta de sua inteligência e acessa os dispositivos com intuito de cometer delitos, inclusive, sem conhecimento tão robusto.

A respeito dos sujeitos nos crimes cibernéticos, é popularmente conhecido dois tipos de agentes criminosos que o praticam, com denominação de sujeito ativo. Isto é, o agente ativo com conhecimento superior de informação quanto à internet e seus sistemas, utilizando-o para praticar o crime típico causando prejuízos aos sujeitos passivos, para obter vantagem a si própria ou terceiros (BARRETO, 2012). Esses sujeitos ativos apenas são conhecidos por dois termos: o hacker e o cracker, o que demonstra que a maioria das pessoas e a sociedade mesmo sendo constantemente alvos de ataques cibernéticos não possui entendimento sobre o assunto.

Além dos popularmente conhecidos, há diversos termos no ambiente virtual para classificar os piratas cibernéticos. Na maioria, possuem características em comum, como são autodidatas, apaixonados por informática, têm conhecimentos em segurança, em auditoria e em ferramentas para quebra de sistema, dentre outras características específicas. Ainda que haja semelhança em algumas características, outras são exatamente o que diferem as terminologias (BACH, 2001).

Assim, há uma grande variedade de nomeações específicas para os sujeitos que praticam os crimes cibernéticos e quanto aos delitos praticados, posto que a sociedade e a área da informação decorrem de grande atualização regularmente. Logo, pode-se verificar que existem diversos termos classificados, contudo, a utilização do termo hacker, de forma facilitada, se torna desvirtuada, de modo que banaliza a questão jurídica do dolo. Termos equivocados e simplificados contribuem para dificultar a compreensão coletiva das referentes dinâmicas no meio da Internet (REZENDE, 2000). Para isso, busca-se diferenciar os termos para completa compreensão.

3.1 DA UTILIZAÇÃO DOS TERMOS HACKER E CRACKER

Embora a maior parte da população conheça o denominado hacker, este não é propriamente o sujeito ativo dos crimes dessa modalidade. Uma vez que, são visualizados com uma negatividade muito maior do que realmente são, pois eles possuem conhecimento de informática e computação, são empenhados em desenvolver e modificar softwares e hardwares de computadores, trabalhando na área de informática e não necessariamente para cometer algum tipo de cibercrime.

Os hackers orientam seu potencial para construir, seu objetivo é compreender mais, não se utilizando do objetivo de destruir ou roubar dados deliberadamente, eles compartilham informações deixando impressões para que administradores de rede realizem correções, pois os verdadeiros hackers são autodidatas, conhecem excessivamente hardware, redes, linguagens de programação, diversos sistemas operacionais, e exatamente os protocolos necessários (BACH, 2001).

Assim, os hackers não devem ser classificados como os criminosos perigosos envolvidos no cibercrime, pois são eles que empreendem o papel da evolução, descobrindo falhas de segurança nos softwares e repassando suas conquistas aos desenvolvedores, ainda auxiliando na reparação. Tal como são eles os responsáveis pela bagagem intelectual na informática, que beneficia todo o meio digital (REZENDE, 2000). Por isso, denominar como hackers aqueles que cometem os crimes cibernéticos, demonstra-se de forma bastante equivocada.

Já os crackers, são os sujeitos que também usam seu

conhecimento, mas buscam o lucro de forma ilícita. Existe uma confusão quanto a classificação desses agentes, ela se deve ao desconhecimento em relação ao assunto, e também por notícias sensacionalistas, que acabam por equiparar as pessoas por seu intelecto informático. O termo cracker foi criado por volta de 1985 pelos próprios Hackers, porque a imprensa empregava o termo "hacker" de forma equivocada para divulgar as ações criminosas realizadas por meio tecnológico (REZENDE, 2000).

Assim, o termo cracker apareceu para designar um grupo de usuários que usaram seu rico conhecimento em informática para violar o sistema de segurança, códigos de criptografia e senhas de acesso à rede, com a intenção de invadir e sabotar para fins criminosos (BACH, 2001). Destaca-se algumas nomeações para cada tipo de delito cibernético, isto é, a forma que utilizaram cometendo esses ilícitos, geralmente derivadas da língua inglesa, com tradução aproximadamente fiel à ação, conforme definições de Coriolano Aurélio de Almeida Carmargo Santos – Diretor de crimes de Alta Tecnologia da OAB:

> Dentre os novos delitos penais cometidos no mundo virtual, os chamados cibercrimes, destacam-se e nomeiam-se alguns a seguir. O "cracking" ou quebra de um sistema de segurança, de forma ilegal e sem ética, por um cracker. O "phishing scam", técnica que permite que piratas virtuais roubem informações de uma máquina com o objetivo principal de burlar transações financeiras. Os atos de "gray hat" e de "black hat". A cor do chapéu define que tipo de ações o hacker pratica. Aquele de "chapéu branco" é um hacker ético. O "black hat" (chapéu preto) é o hacker anti-ético, também denominado cracker. O hacker "gray hat" (chapéu cinza) é aquele penetra um sistema sem, no entanto, lesá-lo, ferir sua confidencialidade ou praticar vandalismo [...]. (SANTOS, 2009, p. 73).

O método utilizado para cometer os cibercrimes, ou seja, de que forma usam de seu conhecimento para cometer alguns dos tipos penais, estão diretamente relacionados com suas nomeações, visto que, existe uma infinidade de crimes cometidos pelo determinado cracker, sejam eles de invasão de sistema de segurança de forma antiética, roubando informações importantes, e principalmente o que acontece com frequência no momento presente, que são os delitos envolvidos em transações financeiras, dado que o meio tecnológico apresenta maior praticidade diariamente.

3. 2 IDENTIFICAÇÃO DOS DIVERSOS SUJEITOS ATIVOS

Têm-se certos termos encontrados para identificar os sujeitos ativos dos cibercrimes, uma vez que não se trata somente dos denominados hackers e crackers. Observa-se uma descrição a respeito dos delitos cometidos pelos crackers, como também, nomeações pouco utilizadas, ou melhor dizendo, realmente pouco conhecidas, aliando-se ao estudo da área de informática que é propriamente mais atualizada, utilizando-se de seus conhecimentos para maior embasamento no direito e tecnologia.

Destarte, o termo Warez que se trata de um indivíduo que aplica os conhecimentos informáticos para copiar programas de forma ilegal e para fins comerciais, algumas de suas atividades são compreendidas nas vendas de programas piratas. Tal como, o termo Wannabe, este é quem sabe combinar algumas técnicas de ataques prontas e invadir sistemas frágeis. Como também, o termo Larva, que consegue desenvolver suas próprias técnicas de ataque e penetrar em sistemas de nível de segurança médio, eles estão considerados na fase de transição entre o wannabe e o hacker. Ademais, a definição de Guru, o perito dos hackers, o máximo de um usuário com habilidades técnicas em todos segmentos (BACH, 2001).

Existem também outras denominações para ações delituosas específicas, como o termo Preaker, para aqueles que burlam os sistemas de telefonia (SPYMAN, 2002). Bem como, o termo Lammer, aplicado para as pessoas que não detêm o conhecimento necessário para desenvolverem suas próprias ferramentas e utilizam ferramentas desenvolvidas por outros para realizarem seus ataques, atualmente conhecido também como "script kiddie" e foi o termo depreciativo mais frequentemente usado no final dos anos 1980 e 1990.

> Preaker são aqueles que fraudam os meios de comunicação telefônica, para proveito próprio sem o pagamento devido, instalando escutas a fim de facilitar o acesso externo, visando o ataque a sistemas. No caso dos Lammers são aqueles que ele possuem algum conhecimento querem se tornar um hacker, e dessa maneira ficam invadindo e perturbando os sites, em outras podem ser denominados de iniciantes. (WENDT; JORGE, 2012, online).

Há os Defacers, a palavra defacer é oriunda do inglês (defacing) e é utilizada para caracterizar aqueles que desfiguram sites ou perfil de redes sociais. Os defacers são semelhantes a pichadores, no entanto, suas atividades são realizadas em sites (WENDT; JORGE, 2013, p. 26). Há também, os Carders, que são especialistas em fraudes por meio de cartões de crédito, os Scammers, que são aqueles que se aproveitam de mensagens enganosas e propagandas falsas levando o sujeito passivo a fornecer informações sigilosas ou instalar softwares de espionagem (SPYMAN, 2002).

Logo, diante dos crimes cibernéticos, há uma grande variedade de nomeações específicas para os sujeitos que o praticam, buscando-se classificar os sujeitos ativos de acordo com as terminologias empregadas no ambiente virtual, evidenciando suas características, habilidades e quanto aos delitos praticados, posto que a sociedade e a área da informação decorrem de grande atualização regularmente, sendo necessária devida atuação legislativa para responsabilizá-los.

4 A RESPONSABILIDADE PENAL DO OFENSOR NA LEGISLAÇÃO PÁTRIA

O processo evolutivo da legislação acerca dos crimes cibernéticos se dá de forma lenta, existindo uma dificuldade de acompanhar a sociedade e sua constante mudança concomitantemente com os delitos informáticos. Mostra-se que a legislação brasileira ainda não acompanha com agilidade, isto é, da mesma forma que acontece a expansão dos cibercrimes, pois sendo a rede mundial de computadores sua ferramenta principal, que se apresenta em grande evolução, há uma discrepância em relação a sua repreensão.

> O Direito Penal encontra muitas dificuldades de adaptação dentro deste contexto. O Direito em si não consegue acompanhar o frenético avanço proporcionado pelas novas tecnologias, em especial a Internet, e é justamente neste ambiente livre e totalmente sem fronteiras que se desenvolveu uma nova modalidade de crimes, uma criminalidade virtual, desenvolvida por agentes que se

> aproveitam da possibilidade de anonimato e da ausência de regras na rede mundial de computadores. (PINHEIRO, 2009, p. 8).

Como o cometimento dos crimes virtuais acontece rapidamente, ainda que seja possível observar um certo avanço, dado que anteriormente nem existia legislação que oferecesse amparo suficiente tratando especificamente dos delitos. Não obstante, os responsáveis por solucionar e punir essas práticas não conseguem acompanhar essa dinâmica evolução, desse modo, mesmo diante do crescimento de vítimas desses crimes, ainda é escasso o número de pessoas punidas por cometê-los, tendo adversidades encontradas na atuação dos órgãos estatais responsáveis pela investigação, identificação e punição dos cibercrimes. Como exemplifica o Professor Fabrízio Rosa sobre a legislação penal (2005, p. 73):

> Não resta dúvida de que a criminalidade informática, infelizmente, é uma manifestação da atualidade, que deve ser combatida. A discussão centra- se em torno das modalidades técnicas de previsão, em referência à dúvida de se abrir caminho a uma legislação especial e autônoma ou então a medidas que inserissem as disposições incriminadoras no corpo do velho Código Penal de 1940, ora vigente. Não resta dúvida de que a Internet é um meio novo de execuções de crimes "velhos", contidos no Código Penal; entretanto, esses crimes não são considerados "crimes de Informática". Estelionato é sempre estelionato, praticado com assistência do computador ou sem ela; afirmar que alguém cometeu um fato definido como crime, sem que tal seja verdade, configura delito de calúnia (Código Penal, art. 138), tanto quando a difusão é feita oralmente ou pelos caminhos da Internet. No entanto, como já salientado, não se deve confundir um crime comum praticado pelo uso ou contra o computador com um "crime de Informática" propriamente dito. Assim, ao formular uma nova categorização, o legislador atrai a atenção da indústria, do mundo acadêmico e do governo para o fato em si que, então, se torna objeto de aprofundamentos novos, os "crimes de Informática", até então desconhecidos pelo legislador penal pátrio de 1940, surgidos com o advento do computador e da Internet.

Dessa forma, amparar-se apenas do Código Penal para a repreensão dos cibercrimes, mostra-se ultrapassado, contudo, segue até o momento como principal dispositivo para tal, pois seus cometimentos estão descritos nos tipos penais anteriormente já implantados. Logo, diante do avanço, e o ajustamento legislativo ao longo dos anos, há uma junção de dois ramos do Direito que identifica a modalidade desses crimes. Tratando-se do Direito da Informática, assim, Rosa diferencia as áreas da seguinte forma (2005, p. 26):

> [...] pode-se definir o chamado Direito de Informática em dois ramos principais: o Direito Civil da Informática e o Direito Penal da Informática. No âmbito concernente ao Direito Civil da Informática, este passaria a concentrar seus estudos no conjunto de normas que regulariam as relações privadas que envolvem a aplicação da Informática, quais sejam: computadores, sistemas, programas, cursos, direitos autorais, documentos eletrônicos, assinaturas digitais etc. Já no que se refere ao Direito Penal da Informática, este seria o conjunto de normas destinadas a regular a prevenção, a repressão e a punição relativamente aos fatos que atentem contra o acesso, uso, exploração, segurança, transmissão e sigilo de dados armazenados e de sistemas manipulados por estes equipamentos, os computadores.

Os estudiosos da área afirmam que tais delitos com uso da Internet podem ser enquadrados na atual legislação penal extravagante, bem como no Código Penal. A assertiva se dá pelo argumento que a Internet é o meio pelo qual se executam esses cibercrimes (SANTOS, 2010, p. 33). Assim, instruída a persecução penal, mediante a investigação do cibercrime cometido, é imprescindível a identificação imediata do meio pelo qual o crime foi praticado, para nortear a ação do órgão investigativo, à medida que serão distintas as técnicas utilizadas para obtenção da autoria e materialidade do crime.

Um dos problemas mais complexos é a prova de autoria do delito na investigação dos crimes cibernéticos, em virtude do anonimato do usuário da rede, pois raramente o sujeito ativo utiliza sua identidade legítima. Isso é o que torna os logs, os eventos que são praticados em determinado acesso e são registrados no sistema computacional, permitindo a verificação dos atos praticados naquele momento e o endereço IP (internet protocol), que refere-se ao registro criado toda vez que uma conexão é feita, essas são as evidências de maior relevância na investigação, além de serem as provas que irão conduzi-las, todavia, obter esses dados é um processo árduo, devido as exigências legais que devem ser respeitadas rigorosamente.

4.1 NOVAS LEIS PENAIS NO ORDENAMENTO BRASILEIRO

Destarte, observa-se o maior dos avanços legislativos no tocante ao tratamento do cibercrime, a Lei 12.737/2012, tomando relevância e publicidade com o nome de Lei Carolina Dieckman. Visto que, até a criação da lei acima citada, havia grande deficiência na tipificação desses delitos, pois até o ano de 2012, a internet era isenta de regulamentação jurídica específica e em virtude disso, se tornou meio fácil para prática de cibercrimes. Entretanto, mesmo sendo um grande avanço, atualmente já apresentava fragilidade sendo alvo constante de críticas (ANDRADE; BENTES; GUIMARÃES, 2017).

Além disso, com a entrada em vigor das leis acima citadas, o artigo 154-A do Código Penal prevê que a ferramenta passou a tipificar o crime de Invasão de Dispositivo Informático, que seria invadir dispositivo informático alheio, conectado ou não à rede de computadores. Contudo, recentemente sofreu alteração, com redação modificando o Código Penal sendo agravadas suas penas em crimes de invasão de dispositivo informático, fraude, furto e estelionato com o uso de dispositivos eletrônicos ou pela internet, em razão do alto cometimento de crimes cibernéticos e sua ineficiente repreensão anterior, veja-se a nova redação alterando o que antes a pena aplicável era de detenção de três meses a um ano e multa, consoante a nova Lei n° 14.155/2021, de 27 de maio de 2021, em seu 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. (BRASIL, 2021, art. 154-A).

Diante do cibercrime e a atuação legislativa, a nova pena passou a ser de um ano e quatro meses de prisão e multa. Tal como, no Decreto-Lei nº 3.689, de 3 de outubro de 1941, o Código de Processo Penal, para definir a competência em

modalidades de estelionato. De acordo com o advogado especialista em Direito Digital, professor da Fundação Getúlio Vargas (FGV) e Presidente da Comissão Nacional de Cibercrimes da Associação Brasileira dos Advogados Criminalistas, Luiz Augusto D'urso, preconiza: "Importante alteração ocorre com esta nova lei, pois acompanhamos um crescimento exorbitante das invasões e golpes pela Internet, principalmente durante a pandemia. [...] Agora, com este aumento, nota-se uma resposta penal muito mais proporcional".[3]

Enquanto em 2014, foi aprovado o Marco Civil da Internet, a Lei nº 12.965/2014, mais tarde conhecido como Constituição Brasileira da Internet, introduzindo sistematicamente os dez princípios formulados pelo Comitê Gestor da Internet no Brasil. Um dos objetivos do Marco Civil é definir legalmente os direitos decorrentes do uso da Internet e estipular o que pode ou não ser feito na área cível antes de criminalizar ações na Internet (BRASIL, 2014). Por isso, a Lei do Marco Civil foi até certo ponto produzida por um movimento de oposição ao projeto de crimes na Internet que tramitavam no Congresso Nacional e que conduziram na criação da Lei 12.737/2012.

Vale ressaltar que os dados de acesso à rede devem ser registrados pelos servidores dos provedores de acesso e de conteúdo através dos logs. Dessa forma, com a criação do Marco Civil da Internet, foi estabelecido o prazo de 06 (seis) meses para que os provedores armazenassem os registros de acesso, devendo mantê-los sob sigilo, podendo ser relativizado mediante ordem judicial de quebra de sigilo de dados, por autoridade judiciária competente (VALVERDE, 2010). Isto posto, importante destacar as demais legislações a nível interno, nível internacional e outras providências em relação ao cibercrime.

4.2 LEGISLAÇÃO INTERNA E INTERNACIONAL SOBRE O CIBERCRIME

Em 2001, foi proposto um tratado internacional de direito penal e direito processual firmado no âmbito do Conselho da Europa, sendo a Convenção de Budapeste, ou então Convenção sobre o Cibercrime, possuindo o objetivo de encontrar formas de persecução aos crimes praticados através da internet, propondo-se uma colaboração internacional entre os Estados-membros, para deter a ação dos ofensores em suas condutas transnacionais com a adoção de uma política criminal comum, entrou em vigor no ano de 2004 e atualmente possui 62 Estados Partes (CONTE, 2008).

Conquanto foi inicialmente organizada para definir e equilibrar as normas de direito penal e processual penal referentes aos cibercrimes cometidos dentro da jurisdição dos Estados-membros do Conselho da Europa, ajustou-se também convidar Estados não membros, a partir de formalização enviada pelo Comitê de Ministros do Conselho da Europa. Em dezembro de 2019 o Brasil foi convidado a aderir após iniciativa do Ministério da Justiça e Segurança Pública. A demanda pela adesão do Brasil vem agregar à Lei 12.965/2014, visando suprir a necessidade de um marco proporcional na área criminal que dê conta da delimitação de parâmetros de persecução penal para tais crimes que, ultrapassam as fronteiras geográficas (BRASIL, 2019).

Há também outras providências, como a criação da SaferNet Brasil, de iniciativa privada, sendo uma organização não governamental, frente à Central Nacional de Denúncias de Crimes Cibernéticos, aplicada em parceria com o Ministério Público Federal, oferece à sociedade e à comunidade internacional um serviço anônimo de recebimento, processamento, encaminhamento e acompanhamento online de denúncias sobre qualquer crime ou violação aos Direitos Humanos praticado através da Internet, apresentando também dados seguros em relação aos diversos cibercrimes (MORAES, 2011).

Logo, a legislação brasileira opera no sentido de garantir meios para que o autor de determinada conduta ilícita possa ser devidamente identificado e responsabilizado por elas, porém, ainda caminha vagamente. Atentando-se que a legislação em geral até este momento não garante completamente meios coercitivos para posteriormente ter a correta identificação do sujeito ativo e respectivo usuário da rede que deu ensejo ao fato violador de direitos, apesar dos recentes ajustes analisados que podem ser verificados futuramente (MORAES, 2011).

Nesse sentido, é por meio da doutrina e jurisprudência que se criam teses para que os provedores de acesso ou de conteúdo sejam responsabilizados nos casos em que não puder identificar o autor, bem como ocorre a atividade de ajustamento da legislação pátria em relação a penalidade dos responsáveis pelos crimes cibernéticos, que decorre constantemente de modernização e incremento.

5 CONSIDERAÇÕES FINAIS

Quando se iniciou o trabalho de pesquisa verificou-se que visava expandir o conhecimento da figura do sujeito ativo que pratica o cibercrime, visto que a realidade é uma constante evolução tecnológica junto à globalização, de forma que todos dependem de dispositivos eletrônicos conectados à rede de internet, por isso era de suma importância estudar sobre os sujeitos ativos do cibercrime e a responsabilidade penal do ofensor, pois estes afetam diretamente a coletividade, uma vez que todos podem ser sujeitos passivos dos crimes cibernéticos, que utilizam demasiadamente do ambiente virtual, sendo relevante para a ciência jurídica, propiciando conhecimento para que compreendam que é possível definir quem comete essas práticas e que existe amparo legislativo.

Diante disso, a pesquisa teve como objetivo geral estudar os sujeitos ativos e os aspectos jurídicos penais do cometimento de crimes cibernéticos no direito brasileiro, constatando-se efetivamente que o trabalho conseguiu identificar os mais importantes e atuais movimentos no meio informático, bem como analisar as diversas complicações para evoluir equivalente a estes, contudo não seria suficiente diante da amplitude do problema.

O objetivo específico inicial era buscar descrever o surgimento da internet para o alcance da perfeita análise do crime em estudo, que foi atendido pela completa análise do advento da mesma, sendo meio idôneo para a prática do comentimento de cibercrimes, bem como compreender a origem e particularidades conceituais do cibercrime, sendo analisados e ressaltados alguns conceitos acerca do tema de maneira ampla, visto que são inúmeras as práticas do

[3] Entrevista de Luiz Augusto Filizzola D'Urso, transcrita no portal Olhar Digital, 28 de maio de 2021.

referido crime cibernético. Já o terceiro objetivo específico era demonstrar a responsabilidade penal diante do cometimento dos cibercrimes à luz do direito brasileiro, que foi permitido diante das criações legislativas até o presente momento, tal como as respectivas atualizações que acompanham o aumento e evolução dos crimes virtuais.

A pesquisa partiu da hipótese de que para responder quem são os sujeitos dos crimes cibernéticos e como podem ser responsabilizados, é importante verificar que estes não são comumente conhecidos pela coletividade no geral, o que resulta demasiadamente na problemática de responsabilizar os autores dos ilícitos, pressupondo-se justamente do aparente obstáculo das investigações para identificá-los e da ausência de evolução constante do processo legislativo para puní-los adequadamente. Durante o trabalho verificou-se que houve preocupação para amenizar os problemas decorrentes do cibercrime, contudo, ainda não são significativas as mudanças para melhorá-los, uma vez que se trata de uma tarefa árdua, porém extremante comum e impossível de ser totalmente solucionada.

Assim, é inegável que a tecnologia se desenvolve instantaneamente e se torna imprescindível aos diversos setores. Devendo então, atentar-se aos impactos que a tecnologia causa na sociedade, tratando-se tanto da evolução do ambiente virtual e da facilidade desta na vida geral, seja também, do lado negativo, como a criminalidade virtual e seu aumento constante, à vista disso que surgiram dispositivos legislativos internos e internacionais com o objetivo de harmonizar as legislações para combater o cibercrime. Logo, demonstra-se que se trata de um evento complicado, que necessita de cooperação internacional daqueles que tutelam esses crimes, como também de conhecimento daqueles que sofrem com isso, justamente por todos serem possíveis sujeitos passivos em razão da utilização da tecnologia que se mostra indispensável.

As entidades investigativas devem possuir maior atenção neste tema, tal como devem dispor de meios que possibilitem maior evolução para abrandar o problema do cibercrime e progredir em sua redução, a nível interno diante da evolução da legislação. Além disso, a prevenção do cibercrime deve aliar-se também a instrução da sociedade no geral, alertando-se para as condutas ilegais que ocorrem na internet mediante o conhecimento das práticas de alguns sujeitos que podem ser definidos de acordo com seus métodos, assim como a existência de meios de defesa que podem proporcionar uma prevenção mais adequada, pois no momento o cibercrime só tende a crescer, contudo ainda pode ser contestado se a sociedade for instruída neste segmento da internet.

REFERÊNCIAS

ANDRADE, Mariah Dourado de; BENTES, Dorinethe dos Santos; GUIMARAES, David Franklin da Silva. Considerações sobre a aplicabilidade do direito penal acerca dos crimes virtuais. **Revista Vertentes do Direito**. Disponível em: https://sistemas.uft.edu.br/periodicos/index.php/direito/article/view/4171#:~:text=O%20presente%20artigo%20busca%20compreender,Leis%20Penais%20regulando%20esse%20crime. Acesso em: 06 abr. 2021.

BACH, Sirlei Lourdes.**Contribuição do hacker para o desenvolvimento tecnológico da informática**. 2001. 135f. Dissertação (Mestrado em Ciência da Computação). Universidade Federal de Santa Catarina Programa de Pós-Graduação em Ciência da Computação. Florianópolis, 2001. Disponível em: http://repositorio.ufsc.br/xmlui/handle/123456789/82176. Acesso em: 18 maio 2021.

BARBAI, Marcos Aurélio. A criminalidade no espaço digital: a formulação do sentido. In. DIAS, Cristiane. **Formas de mobilidade no espaço e-urbano**: sentido e materialidade digital [online]. (Série e-urbano, v.2), 2013. Disponível em: https://www.labeurb.unicamp.br/livroEurbano/. Acesso em: 26 maio 2021.

BARRETO, Erick Teixeira. **Crimes cibernéticos sob a égide da Lei 12.737/2012**. Revista Âmbito Jurídico. Disponível em: https://ambitojuridico.com.br/edicoes/revista-159/crimes-ciberneticos-sob-a-egide-da-lei-12-737-2012/. Acesso em: 20 dez. 2020

BRASIL. **Decreto-Lei nº 2.848, de 07 de dezembro de 1940**. Código Penal. Rio de Janeiro. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 19 dez. 2020.

BRASIL. **Decreto-Lei nº 3.689, de 03 de outubro de 1941**. Código de Processo Penal. Rio de Janeiro, Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 12 jun. 2021.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. [S. l.], 1 set. 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 20 dez. 2020.

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. [S. l.], 1 set. 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm. Acesso em: 18 dez. 2020.

BRASIL. **Lei n° 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. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Lei/L14155.htm. Acesso em: 07 jun. 2021.

BRASIL. Ministério das Relações Exteriores. **Nota à imprensa n° 309/2019**. Processo de adesão à Convenção de Budapeste - Nota Conjunta do Ministério das Relações Exteriores e do Ministério da Justiça e Segurança Pública. Disponível em: https://www.gov.br/mre/pt-br/canais_atendimento/imprensa/notas-a-imprensa/2019/processo-de-adesao-a-convencao-de-budapeste-nota-conjunta-do-ministerio-das-relacoes-exteriores-e-do-ministerio-da-justica-e-seguranca-publica. Acesso em: 11 jun. 2021.

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: https://egov.ufsc.br/portal/conteudo/crimes-virtuais-elementos-para-uma-reflex%C3%A3o-sobre-o-problema-na-tipifica%C3%A7%C3%A3o/. Acesso em: 08 abr. 2021.

CONTE, Christiany Pegorari; SANTOS, Coriolano Aurélio De Almeida Camargo. Desafios do Direito Penal no Mundo Globalizado: A aplicação da Lei Penal no espaço. **Revista de Direito de Informática e Telecomunicações**, ISSN 1983-392X, 2008.

COMISSÃO EUROPEIA. Digital Privacy. European Commission. Disponível em: https://ec.europa.eu/digitalsingle-market/en/policies/online-privacy. Acesso em: 20 maio 2021.

CONVENÇÃO SOBRE O CIBERCRIME. Budapeste, 2001. Disponível em: http://www.mpf.mp.br/atuacaotematica/sci/normaselegislacao/legislacao/legislacoespertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf. Acesso em: 7 de jun. 2021.

D'URSO, Luiz Augusto Filizzola. Sancionada lei que endurece penas para crimes cibernéticos. [Entrevista cedida a] Karol Albuquerque. **Olhar Digital**. São Paulo, 28 maio 2021. Disponível em: https://olhardigital.com.br/2021/05/28/seguranca/sancionada-lei-que-endurece-penas-para-crimes-ciberneticos/. Acesso em: 05 jun. 2021.

FRANÇA, Leandro Ayres; QUEVEDO, Jéssica Veleda; FONTES, Jean de Andrade; SEGATTO, Anderson José da Silva; ABREU, Carlos Adalberto Ferreira de; SANTOS, Diego da Rosa dos; VIEIRA, Luana Ramos. "Projeto Vazou: pesquisa sobre o vazamento não consentido de imagens íntimas no Brasil". **Revista Brasileira de Ciências Criminais**, v. 169, ano 28. p. 231-270. São Paulo: RT, jul. 2020. ISSN 1415-5400.

JUNIOR, Júlio Cesar Alexandre. Cibercrime: um estudo acerca do conceito de crimes informáticos. **Revista Eletrônica da Faculdade de Direito de Franca**. Disponível em: https://www.revista.direitofranca.br/index.php/refdf/article/view/602#:~:text=Cibercrime%20est%C3%A1%20associado%20ao%20%E2%80%9Cfen%C3%B3meno,12). Acesso em: 07 abr. 2021.

MORAES, Paulo Francisco Cardoso de. A vedação constitucional do anonimato aplicada à internet: o papel do estado brasileiro na identificação dos usuários e responsabilização dos provedores. **Revista Âmbito Jurídico**. Disponível em: https://ambitojuridico.com.br/edicoes/revista-91/a-vedacao-constitucional-do-anonimato-aplicada-a-internet-o-papel-do-estado-brasileiro-na-identificacao-dos-usuarios-e-responsabilizacao-dos-provedores/. Acesso em: 06 jun. 2021.

NASCIMENTO, Samir de Paula. **Cibercrime:** conceitos, modalidades e aspectos jurídicos-penais. Disponível em: https://ambitojuridico.com.br/cadernos/internet-e-informatica/cibercrime-conceitosmodalidades-e-aspectos-juridicos-penais/. Acesso em: 19 dez. 2020.

NUCCI, Guilherme de Souza. **Manual de direito penal.** 10. ed. rev., atual. e ampl. Rio de Janeiro: Forense, 2014.

PINHEIRO, Emeline Piva. **Crimes virtuais:** uma análise de criminalidade informática e da resposta estatal. Disponível em: https://egov.ufsc.br/portal/conteudo/crimes-virtuais-uma-an%C3%A1lise-da-criminalidade-inform%C3%A1tica-e-da-resposta-estatal-0. Acesso em: 17 dez. 2020.

REZENDE, Pedro Antonio Dourado de. **Tópicos em Segurança de Dados**. Universidade de Brasilia - UNB. Disponível em: http://www.cic.unb.br/docentes/pedro/pedro.html. Acesso em: 24 maio 2021.

ROQUE, Sérgio Roque. **Criminalidade Informática – Crimes e Criminosos do Computador**. São Paulo: ADPESP Cultural, 2007.

ROSA, Fabrízio. **Crimes de Informática**. Campinas: Bookseller, 2005.

SANTOS, Coriolano Aurélio De Almeida Camargo. **As múltiplas faces dos Crimes Eletrônicos e dos Fenômenos Tecnológicos e seus reflexos no universo Jurídico**. São Paulo: OAB SP, 2009.

SANTOS, Coriolano Aurélio De Almeida Camargo; FRAGA, Ewelyn Schots. **As múltiplas faces dos Crimes Eletrônicos e dos Fenômenos Tecnológicos e seus reflexos no universo Jurídico**. 2. ed. São Paulo: OAB SP, 2010.

SILVA, Paulo Quintiliano da. **Dos Crimes Cibernéticos e seus efeitos internacionais**. Procedings of the Firts International Conference on Forensic Computer Science Inv estigation (ICoFCS´2006)/ Departamento de Polícia Federal (ed.) Brasília, Brazil, 2006,124 pp.- ISSN 19180-1114

SIMAS, Diana Viveiros de. **O cibercrime**. 2014. 168f. Dissertação (Mestrado em Ciências JurídicoForenses). Universidade Lusófona de Humanidades e Tecnologias. Lisboa, 2014. Disponível em: http://hdl.handle.net/10437/5815. Acesso em: 18 maio 2021.

SOUZA, Henry Leones De. VOLPE, Luiz Fernando Cassilhas. **Da ausência de legislação específica para os crimes virtuais**. Disponível em: https://egov.ufsc.br/portal/conteudo/da-aus%C3%AAncia-de-legisla%C3%A7%C3%A3o-espec%C3%ADfica-para-os-crimes-virtuais. Acesso em: 08 abr. 2021.

SPYMAN. **Manual Completo do Hacker**. Rio de Janeiro, RJ, 2002.

VALVERDE, Danielle Novaes de Siqueira. Crimes

Cibernéticos: a obrigatoriedade do registro de acesso à internet como forma de possibilitar a identificação do criminoso. **Revista da ESMAPE**. Recife. v. 15. n. 32. p. 245. jul./dez. 2010.

WENDT, Emerson; JORGE, Higor Vinícius Nogueira. **Crimes cibernéticos:** Ameaças e procedimentos de investigação. Rio de Janeiro: Brasport, 2012.