



O PROCESSO LEGIFERANTE NA ÉDGE DOS CRIMES DIGITAIS

THE LAWSUIT PROCESS AT THE EDGE OF DIGITAL CRIMES

DOI: 10.5281/zenodo.8353677

Jefferson Florencio Rozendo¹

Francisco Apoliano Albuquerque²

Thiago Luís de Oliveira Albuquerque³

RESUMO: O trabalho tem como foco demonstrar fatos relacionados a crimes cibernéticos ou cybercrimes. Assim como, apresentar a insuficiência de tipificações com cunho de punir crimes virtuais, analisar o uso das mídias sociais nos crimes digitais, bem como, contextualizar a historicidade da internet, avaliar a ação penal e a apuração dos delitos informáticos. Para a concretude deste trabalho, realizamos a pesquisa de revisão de literatura. Verificou-se a tal pendência jurídica faz com que pessoas com má índole, com conhecimentos mais aprofundados na arte de programação os denominados crackers ou mesmo com diminutos conhecimentos, passam a produzir ações de cunho danoso, nas modalidades de crimes contra a honra, divulgação de informações pessoais. Os resultados revelaram emergentes necessidades, a criação de leis severas se faz necessária para a erradicação destes delitos, pois os agentes causadores do delituoso deixam de ser responsabilizados dos malefícios causados. Concluimos diante a divulgação, incorporados a mensuração das poucas leis atuais e aplicadas, o trabalho, deseja uma expectativa panorâmica de questões coligadas aos ilegítimos realizados por interposição da Internet com as leis vigentes.

Palavras-chave: Crimes Virtuais, Crimes Digitais, Legislação.

ABSTRACT: The paper focuses on demonstrating facts related to cybercrime or cybercrime. As well as presenting the insufficiency of typifications to punish cybercrimes, analyzing the use of social media in digital crimes, as well as contextualizing the historicity of the internet, evaluating the

- 1 Doutorando em Ciências da Educação (ACU), Mestre em Educação Profissional e Tecnológica (PROFEPT). Instituto Federal de Educação Ciência e Tecnologia do Ceará, IFCE.
- 2 Pós-Dótor em direito penal e as garantias constitucionais pela universidade de La Matanza - Bueno Aires – Argentina. Mestrado em Gestão Pública Estadual e Municipal pela Universidade Estadual Vale do Acaraú, em parceria com a Universidade Internacional de Lisboa Doutorado em Administração de Empresas pela Universidad Americana.
- 3 Doutorando em Direito – UNIMAR - SP



criminal action and the investigation of computer crimes. For the concreteness of this work, we conducted the literature review research. It has been found that such legal pending causes people with bad character, with deeper knowledge in the art of programming the so-called crackers or even with little knowledge, start producing actions of harmful nature, in the modalities of crimes against honor, disclosure of information. People information. The results revealed emerging needs, the creation of severe laws is necessary for the eradication of these crimes, as the causative agents of the offender are no longer held responsible for the harm caused. We conclude from the disclosure, incorporating the measurement of the few current and applied laws, the paper, wants a panoramic expectation of issues related to illegitimate carried out by interposition of the Internet with the laws in force.

Key words: Virtual Crimes, Digital Crimes, Legislation

1 INTRODUÇÃO

Este estudo se insere na área de crimes cibernéticos e tem como temática a análise: O processo legiferante na édige dos crimes digitais.

A opção por essa temática deve-se ao fato de estar vinculada, com o Programa de Graduação em Direito pela FAECE/FAFOR, logo, instigou-me produzir esse trabalho monográfico.

Nessa perspectiva, este estudo está inserido nos crimes cibernéticos, incorporada nas Novas Tecnologias. Visto que, nos dias atuais, já acordamos com significativas mudanças e atualizações junto aos meios de comunicação. Despertando questionamentos ligados a quem realmente somos e até onde podemos seguir, na qualidade de partícipes de um mundo, que até pouco tempo, cerca de 40 anos nos era totalmente, não sonhado?

A problemática está inserida na utilização das mídias sociais com a prática de crimes digitais que tem se tornado, cada vez mais frequente nos últimos anos. Por essa razão, a fim de contribuir para aprofundar o conhecimento sobre o uso das mídias sociais em processos cibernéticos.

Tal questionamento conduz a uma discussão sobre o papel das mídias digitais como ferramentas de apoio aos crimes digitais em um mercado em desenvolvimento, tendo em vista o avanço significativo do número de pessoas com acesso à Internet.



Tendo como objetivo central deste estudo compreender uso das mídias sociais nos crimes digitais. Especificamente, contextualizar a historicidade da internet, avaliar a ação penal e a apuração dos delitos informáticos.

O presente estudo buscou resposta à seguinte indagação: De que forma o uso das mídias sociais deram suporte ao processo legiferante na édige dos crimes virtuais? Analisar o uso das mídias sociais nos crimes digitais, bem como, contextualizar a historicidade da internet, avaliar a ação penal e a apuração dos delitos informáticos.

Esse estudo está organizado em 3 capítulos, além da introdução e das considerações finais. Nos quais, buscamos respostas para atender os objetivos traçados. Sendo assim, está distribuída de forma, a saber, na qual investigamos: Como surgiram os crimes cibernéticos, termos usados a toda a atividade criminosa em que se utiliza um computador ou uma rede de computadores como instrumento ou base de ataque?

O capítulo um aborda dados referentes ao contexto da investigação como: Estudos recentes sobre INTERNET, abordagem pertinente a internet e crimes virtuais no tempo, pesquisas em sites em internet, revistas especializadas, Dissertação de Mestrado, legislações, Decretos que apresentam os referidos crimes. Realizamos uma abordagem teórica sobre a origem histórica e definições da rede mundial de computadores, aspectos internet.

O capítulo dois apresenta a criminalidade na rede, bem como, a classificação doutrinária dos crimes cibernéticos, os delitos virtuais próprios, os delitos virtuais impróprios, sujeitos ativos e sujeitos passivos.

O capítulo três aborda a investigação e análise apresentando os resultados inerentes à pesquisa, visando à compreensão do fenômeno investigado. A pesquisa traz algumas reflexões que poderão levantar outras provocações acerca do fenômeno crimes cibernéticas,



bem como prováveis desdobramentos vindos deste estudo contribuindo no campo da Ciência.

O estudo é da modalidade revisão de literatura, no qual buscamos examinar as relações dos crimes cibernéticos. A pesquisa foi realizada por meio de levantamentos bibliográficos e dos principais artigos científicos, bem como legislações publicadas a partir de 2006 e as mais recentes. Além desses, foram utilizados livros, dissertações, teses e a estruturação conceitual do referencial teórico do trabalho monográfico (GUERRA, 2023).

2 MARCO DA INTERNET

Este capítulo apresenta estudos sobre o surgimento da INTERNET pertinentes ao contexto virtual de idéias e informações, fundamentados em pesquisas através de revistas especializadas na temática, Dissertação de Mestrado, legislações, Documentos dos quais expõem os crimes virtuais no tempo, bem como, uma abordagem teórica sobre seu avanço histórico e legalístico no Brasil.

Neste contexto, destaca-se que a internet surgiu em meio ao período da Guerra Fria, no final da década de 50 incorporando o desenvolvimento tecnológico ao militar de forma marcante, visto que os países se preparavam militarmente para uma provável confrontação armada. Neste cenário, atuações de investigação e técnicas de aquisição de informação se tornaram constantes.

Dessa forma, o serviço de inteligência passou a ser estratégico, aliado a informática. Neste sentido, os anos da Guerra Fria apontaram o progresso desse escopo, usando os computadores como ferramentas de comunicação e influência de informações (EDWARDS, 1996).



A princípio a intenção seria conectar os mais renomados centros universitários de pesquisa americanos com o Pentágono para possibilitar a correspondência de informações instantâneas e resguardadas, do mesmo modo, operacionalizarem o país como uma técnica que permitisse a sobrevivência de caminhos de informação, numa possível guerra nuclear.

Os idealizadores do projeto nunca imaginariam que a Internet desenvolveria tanto, quanto se encontra nos dias atuais. A tecnologia usada para transferência de informações foi inventada com a nomenclatura de WAN (Wide Area Networks), mas a linguagem empregada nos computadores conectados em rede era muito complicada, por isso, a potencialidade de propagação da Internet não podia ser concebida (Merkle e Richardson, 2000).

No início da década de 80, a ARPANET ainda era uma rede conectada simplesmente com determinados universidades que tinham convênios com a ARPA. Essas universidades, além de desenvolverem pesquisas com os objetivos militares, precisavam ter a habilidade financeira para encarregar em aparelhamentos e circuitos de comunicação necessários para fazer parte da rede, pois manter um nó da ARPANET custava aproximadamente US\$ 100 mil por ano (HAFNER, 1996, p. 242).

Já no Brasil a internet apareceu a partir da década de 90, sendo oferecidas para pesquisas, em determinadas universidades, estas só poderiam usar para com a finalidade de pesquisas. Em 1994 a internet iniciou a sua comercialização, sendo distribuída pela empresa de telecomunicação Embratel. Em 1995 o Ministério das Telecomunicações em unido com o Ministério da Ciência e Tecnologia, iniciaram as atividades para oportunizar o acesso à internet para a sociedade brasileira.

A internet mantém-se conectado ao computador no qual a pessoa acessa o portal para obter informações no espaço cibernético, que compreende um mundo virtual de conceitos e informações em que adentramos para lermos utilizando um computador.



Em meio a isso, é chamada por “web” a forma que permite “manejar” as dados na internet. “[...] É um sistema de documentos dispostos na Internet que permitem o acesso às informações apresentadas no formato de hipertexto. Para ter acesso a tais informações pode-se usar um programa de computador chamado navegador” (MARTINS, 2008).

No período que abrangeu o fim da “Guerra Fria”, a Internet, deixou de ser importante para os militares, que potencializaram as pesquisas nas universidades, já em curto prazo, estenderam o acesso ao programa a pesquisadores domésticos, isso em virtude do avanço de indicadores de usuários. Assim, como cresceu a celeridade nos avanços tecnológicos, as ameaças virtuais medidas pela informática foram surgindo.

Soma-se, a isso, um grupo de programadores organizaram um jogo designado “Core Wars”, com a particularidade de se auto reproduzir a cada desempenho, ocasionando um sobrepeso à memória do computador. Estes especialistas programadores, ao mesmo tempo, criaram o primeiro antivírus, chamado de “Repper”, com a intenção de extinguir as imitações inventadas pelo “Core Wars”.

Após este acontecimento, umas variantes de intimidações surgiram com o uso de computadores. Para delinear a ocorrência, citamos o jovem Richard Skrenta, que, aos quinze anos, produziu o “ElkCloner”, qualificado por vários estudiosos como o primeiro vírus com a finalidade de infectar computadores.

Atualmente, muitos desses tipos de crime, não se limitam apenas ao campo computacional, ocasionando danos só nos aparelhamentos, mas do mesmo modo, em alguns casos, invadindo o íntimo de certas pessoas, cita-se, a invasão ao iCloud de famosos, como Jennifer Lawrence, que teve suas fotos divulgadas sem sua devida permissão.

Deste modo, ressaltamos que todos os dias, pessoas têm conteúdos pessoais publicado, assim, sofrendo implicações ilícitas.



3 CRIMES VIRTUAIS

Há vários crimes executados em espaço digitais. Podemos mencionar tais crimes, de computação, delinquência de informática, violação de computador, dolo informática, ainda não há conceitos definidos que abrangem todas as modalidades dos crimes conectados à tecnologia, há muitas ocorrências complicadas no espaço virtual.

Neste sentido, Rosa conceitua o crime de informática como:

A conduta atente contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, seja pela compilação, armazenamento ou transmissão de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar; 2. O ‘Crime de Informática’ é todo aquele procedimento que atenta contra os dados, que faz na forma em que estejam armazenados, compilados, transmissíveis ou em transmissão; 3. Assim, o ‘Crime de Informática’ pressupõe dos elementos indissolúveis: contra os dados que estejam preparados às operações do computador e, também, através do computador, utilizando-se software e hardware, para perpetrá-los; 4. A expressão crimes de informática, entendida como tal, é toda a ação típica, antijurídica e culpável, contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão; 5. Nos crimes de informática, a ação típica se realiza contra ou pela utilização de processamento automático de dados ou a sua transmissão. Ou seja, a utilização de um sistema de informática para atentar contra um bem ou interesse juridicamente protegido, pertença ele à ordem econômica, à integridade corporal, à liberdade individual, à privacidade, à honra, ao patrimônio público ou privado, à Administração Pública, etc (ROSA, 2002, p.54).

Deste modo, os crimes de informática são bem diversificados, eles se apropriam de dados, tanto da conduta pessoal, quanto ao patrimônio público ou privado, à Administração Pública, dentre outros. Tal prática é realizada através de invasão de computadores por meio de vírus já criado com o objetivo ilícito, por especialistas na área. Às vezes, essa prática delituosa é feita com o uso da internet e do computador, em outras situações não é necessário estar conectado com a internet para a realização do delito.



Roque (2007, p. 25), define o crime de informática como “toda conduta, definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material”.

Enquanto isso, o Direito Penal revela que o crime é todo procedimento típico, antijurídico e culpável. Os crimes de informática, designados do mesmo modo, de crimes digitais, virtuais, cybercrimes, são aqueles incumbidos através dos computadores, versus os mesmos, ou por outro através dele próprio.

Dentre os crimes cometidos através da invasão de dados de uma pessoa através de um computador, pode-se furtar todo dinheiro de uma conta bancária, adquirir fotos pessoais com o objetivo de ameaçar a vítima, isso com o interesse de se apossar do dinheiro ou denegrir a imagem da pessoa perante a sociedade.

4 HISTORICIDADE DA REDE MUNDIAL DE COMPUTADORES

A Rede Mundial de Computadores trata-se de um instrumento de informação, cada vez mais, usada no dia-a-dia das pessoas e avaliada por muitos, como algo necessário na prática de trabalhos, além de promover as relações sociais.

Neste contexto, esse instrumento surge recheado com um banco de dados, pode ser analisado como uma fonte preciosa por indivíduos que tenham como finalidade a prática criminosa, às vezes, causando graves detrimientos financeiros e pessoais aos que usam a Internet.

Assim, para Wendt (2014, p.1): “surtem os chamados crimes cibernéticos, caracterizados pela prática de delitos no ambiente virtual ou por intermédio deste”. Nesta condição há existência de previsão legal.



A Internet é um sistema operacional com expansão comunicacional mundial, que oferece uma variedade de programas, recursos, aplicativos disponibilizados aos seus usuários. Algumas das principais atividades advindas da internet são: o acesso a sites de informações, entretenimento, diversão, relacionamentos, bem como acordos comerciais. No entanto, encontram-se nesse meio virtual usuários que a utilizam com interesse meramente delituosos, maléfico à sociedade, assim, tidos como Crimes Virtuais ou cibernética.

De acordo com Chaves (apud SILVA, 2003, p.19), Cibernética é a “ciência geral dos sistemas informantes e, em particular, dos sistemas de informação”. Assim, por meio do conceito analítico de crime, pode-se chegar à conclusão de que “crimes cibernéticos” são todas as condutas “típicas, antijurídicas e culpáveis praticadas contra ou com a utilização dos sistemas da informática” (SCHMIDT, 2014, [n.p.]).

Um ponto que cabe ser destacado, é que a Rede Mundial de Computadores conecta de forma virtual, por meio da internet, pessoas em volta do planeta, sendo considerada a “mãe” de todas as conexões, que se originou de um projeto militar norte americano.

Diante a tal proposta, o governo norte-americano queria desenvolver um sistema para que seus computadores militares pudessem trocar informações entre si, de uma base militar para a outra e que mesmo em caso de ataque nuclear os dados fossem resguardados, isto é, seria uma tecnologia de resistência.

Dessa forma, surgiu a ARPANET, o predecessor da internet, um projeto estreado pelo Departamento de Defesa dos Estados Unidos que realizou a interconexão de computadores, através de um sistema experimentado como permutação de pacotes, que é um plano de difusão de dados em rede de computadores no qual as informações são repartidas em pequenos “pacotes”, que por sua vez contém trecho de dados, o endereço do destinatário e informações que permitiam a remontagem da mensagem original (MONTEIRO, 2009, [n.p.]).



Com o tempo pequenas redes começaram a utilizar a tecnologia desenvolvida pela ARPANET. O estabelecimento do Protocolo de Comunicação (The Internet Protocol-IP) foi o que permitiu a experiência da internet e admitiu que qualquer quantia de computadores fosse interligada em rede (GOUVEIA, 1997).

A internet é considerada um divisor de épocas, unida à historicidade da humanidade, sobretudo, pela quantidade de melhoramentos que permite, mas do mesmo modo, por estar se tornando uma ferramenta de crime, dessa forma, ocasionando as pessoas muitas inquietações.

No cyber espaço tem a dispersão dos atos criminosos que cooperam tanto para a origem de novos delitos, quanto para a efetivação de crimes já experimentados.

5 ASPECTOS POSITIVOS DA INTERNET

Com a capacidade de mudanças constantes no campo da comunicação mundial, onde cada vez mais estão presentes nas mais variadas ações rotineiras, com influencia nos aspectos: econômicos, político, lazer, econômico, investigação, comércio e serviços on-line, educação, enfim, nas mais diversas áreas de nossa realidade estejam você onde estiver.

Quanto à busca de informações, a internet é a preferida entre os usuários. Dentro dela está a World Wide Web (WWW) que, baseando-se em arquivos de hipertexto em uma linguagem chamada HTML e por meio do uso de um protocolo específico (HTTP) onde é possível o compartilhamento de informações, disponibilizando-as à busca por parte dos interessados.

Na concepção de Moran (2003 apud DILLIUS, 2012, [n.p.]): Uma das características mais interessantes da Internet é a possibilidade de descobrir lugares inesperados, de encontrar materiais valiosos, endereços curiosos, programas úteis, pessoas



divertidas, informações relevantes. São tantas as conexões possíveis, que a viagem vale por si mesma.

Nesta perspectiva, a rede precisa de intuição determinada, de estarmos atento para fazer tentativas no escuro, para acertar e errar. A pesquisa nos leva a garimpar jóias entre um monte de banalidades, a descobrir pedras preciosas escondidas no meio de inúmeros sites publicitários.

Conforme Valzacchi (2003), a utilização da internet em aulas pode chegar a ser proveitoso, para ele:

Aprender a aprender e a desenvolver a criatividade são habilidades críticas na sociedade onde o conhecimento se renova com velocidades inesperadas. Através de diálogos entre os pares, entre alunos e professores ou em comunidades de aprendizes (VALZACCHI, 2003, p. 129-177).

É possível acessar informações em qualquer lugar do mundo, onde podemos pesquisar informações em bibliotecas, universidades, livrarias, doutrinadores, entre outros lugares e diversificados temas.

6 CRIMINALIDADE NA REDE

O computador conectado a internet promove benefícios a sociedade, eles também são impulsionados pelas novas condutas de cunho ilícitas, praticadas por criminosos especializados nesse campo.

Essas ações possuem denominações diversas, sendo comumente denominados de crimes virtuais, crimes cibernéticos, digitais, informáticos, telemáticos, de alta tecnologia, crimes por computador, crimes de internet, fraude informática, crimes transnacionais, entre outras.



Neste cenário, temos a figura do criminoso informático, detentor de inteligência, conhecimento de sistemas de informações e usos pertinentes aos meios informatizados com a finalidade de atingir bens jurídicos alheios, fazendo-se valer de um novo universo de possibilidades de atuação criminosa.

O Direito Penal encontra muitas dificuldades para se adaptar a essas ocorrências específicas no cenário dos crimes digitais.

Visto que, o Direito não consegue acompanhar o avanço das novas tecnologias, em particular a Internet, é neste ambiente livre e sem fronteiras que se desenvolveu tal 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 apud DULLIUS, 2012, [n.p.]).

Ainda que seja bastante crítica essa visão conota, que o ciberespaço é um lugar imaginário, que apenas pelo computador temos acesso, mas mesmo assim precisa estar ligado à realidade pelo uso que temos feito dele nos dias atuais, transformando-o em um espaço intermediário entre o mundo imaginário e o mundo real.

Tendo consciência dessa complexidade, Terceiro (2009 apud DULLIUS, 2012, [n.p.]) menciona que os crimes perpetrados neste ambiente se caracterizam pela ausência física do agente ativo, por isso, ficaram usualmente definidos como sendo crimes virtuais, ou seja, os delitos praticados por meio da Internet são denominados de crimes virtuais, devido à ausência de seus autores e seus asseclas.

Verificamos que o crime virtual é qualquer conduta antijurídica e culpável, realizada a partir de um computador conectado à internet.

De acordo com Rossini (2004 apud DULLIUS, 2012, [n.p.]):



[...] o conceito de “delito informático” poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade a confidencialidade (ROSSINI, 2004).

Deste modo, o crime virtual pode ser aquele que perpetra algum ato típico, antijurídico ou culpável, com finalidade de processamento automatizado de dados ou sua difusão em que um computador interligado ou não à rede de computadores de forma mundial. Por conseguinte, a própria invasão, embora não cause dano configura crime.

E ainda em relação a essa situação, vale mencionar que o “delito informático” é gênero, do qual “delito telemático” é espécie, dada a peculiaridade de ocorrer no e a partir do inter relacionamento entre os computadores em rede telemática usados na prática delitiva (ROSSINI, 2004 apud DULLIUS, 2012).

Partindo de uma perspectiva baseada na “Convenção sobre o Cibercrime de Budapeste”, realizada no ano de 2001, pode-se aduzir que os crimes de informática são aqueles perpetrados por meio dos computadores, contra eles ou através deles, de modo que a maioria dos crimes é praticada por meio do sistema de internet (SCHMIDT, 2014 apud CASTRO, 2003).

Ademais, tratando-se de antecedentes históricos, podemos dizer que os aparecimentos dos primeiros casos de crimes informáticos ocorreram na década de 1960, os quais, nada mais eram, do que delitos em que o infrator manipulava, sabotavam, espionava ou exercia abuso abusivo de computadores e sistemas.

Outro fator relevante é que, foi só a partir do ano de 1980, que houve um avanço das ações criminosas, que passaram a pensar em, por exemplo, manipulações de caixas



bancários, abusos de telecomunicação, pirataria de programa e pornografia infantil, sendo que o último fato vem preocupando consideravelmente os cidadãos (OLIVEIRA, 2013).

E em razão dessas situações é importante destacar que o contexto considerado novo no âmbito de Lei é a criminalidade cibernética. Em 3 de dezembro de 2012 foi sancionada a Lei nº 12.737/2012 que aborda o caso, a chamada “Lei conhecida Carolina Dieckmann” a qual promoveu, algumas necessárias inquietações no Código Penal Brasileiro (CPB), tipificando os chamados “delitos ou crimes informáticos”.

É interessante ressaltar ainda que a lei acrescentou os artigos 154-A e 154-B e alterou os artigos 266 e 298 do Código Penal Brasileiro (FRANCESCO, 2014). No Art. 154-A, consta dominar dispositivo informático de outrem, interligado ou não à rede de computadores, mediante violação indevida de organismo de segurança e com o fim de conseguir, falsificar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou construir vulnerabilidades para impetrar vantagem ilícita: (Incluído pela Lei nº 12.737, de 2012) Vigência Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. (Incluído pela Lei nº 12.737, de 2012) vigência.

Outro fator relevante é o Art. 154-B, que constam os crimes definidos no art. 154-A, só se provém mediante representação, salvo se o crime e atentado contra a administração pública direta ou indireta de algum dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos. (Incluído pela Lei nº 12.737, de 2012) Vigência.

Tal legislação foi fruto do Projeto de Lei nº 2793/2011, tramitou em regime de urgência no Congresso Nacional, sobre delitos informáticos que as casas de leis contemplavam (como, por exemplo, o PL 84/1999, a “Lei Azeredo”, do mesmo modo convertido em lei ordinária 12.735/2012 em 3 de dezembro de 2012).



O codinome se deu devido à repercussão do caso no qual a atriz teve seu computador invadido e seus arquivos pessoais subtraídos, até mesmo com a publicação de fotos íntimas que ligeiramente se disseminaram pela internet através das redes sociais (OLIVEIRA, 2013).

É importante enfatizar que os sistemas informáticos têm no atual cenário social, observando que a maioria das pessoas, físicas ou jurídicas, estar sujeito do seu aparelho informatizado, que variam desde um pendrive ou celular, até um computador com banco de dados confidenciais de uma empresa.

É preciso considerar também no que se refere à segurança informática, tratada como a disponibilidade, confidencialidade e integridade das informações dos usuários, já protestavam há tempo, por amparo jurídico-penal, já que a “violência” nesse meio evolui rapidamente.

Em contra partida, a legislação vem enfrentando rigorosas críticas de juristas, peritos, especialistas e profissionais de segurança da informação, pois seus dispositivos são amplos, confusos e podem provocar dupla interpretação, ou mesmo interpretação subjetiva, onde pode ser usado para enquadramento criminal de condutas triviais ou mesmo, para a defesa e respaldo de infratores cibernéticos, o que tornaria a lei injusta e ineficaz.

Assim, os simpatizantes de antagônica corrente, diz que as penas são pouco inibidoras, sendo muitas as ocorrências enquadráveis nos procedimentos dos Juizados Especiais, o que poderia cooperar para a não eficácia na ação ao crime cibernético no Brasil.

Ainda sobre esse texto o desempenho da polícia em crimes de computação, crimes desse caráter demandam investigação especializada e ação efetiva. Infelizmente, não existem no Brasil, policiais preparados para combater esse tipo de crime, faltando, visão, planejamento, investimento, qualificação e treinamento (MIRANDA, 2013).



Acrescente-se, ainda, que, o plano de requinte hackers brasileiros vem crescendo consideravelmente junto com eles, ocasionando prejuízo para as empresas e para os cidadãos numa visão unânime. Estes criminosos digitais permeiam nas áreas de atuação, como roubo de identidade, fraudes de cartão de crédito, violação de propriedade intelectual e protestos políticos, compras online, dentre outros.

Ainda pertencente a essa situação as cópias de software, tidas protegidas por direitos autorais e piratagem, bem como o depredação on-line, são alguns das prática ilícitos cada vez mais adotadas por hackers nacionais.

E em razão dessas situações a evolução da internet e o acrescentamento descomedido da informatização fazem com que os crimes versados pela internet, ao mesmo tempo nomeados “crimes virtuais” sejam cada vez mais comuns e complexos de combater no ordenamento jurídico brasileiro devido à dificuldade de penitenciar de forma dinâmica os agentes devidos, sobretudo, à impressão de impunidade provocada.

7 CATEGORIZAÇÃO DOUTRINÁRIA DOS CRIMES CIBERNÉTICOS

A categorização doutrinária dos crimes cibernéticos é **distribuída** pela doutrina brasileira predominante como delito de natureza formal, visto que se desgastem no momento da prática da conduta delitiva, independente da passagem da decorrência naturalístico.

Ao considerar os referidos aspectos é importante ressaltar, o jurista Maggio (2013, [n.p.]) classificou os crimes cibernéticos. In verbis:

Trata-se de crime comum (aquele que pode ser praticado por qualquer pessoa), plurissubsistente (costuma se realizar por meio de vários atos), comissivo (decorre de uma atividade positiva do agente: “invadir”, “instalar”) e, excepcionalmente, comissivo por omissão (quando o resultado deveria ser impedido pelos garantes – art. 13, § 2º, do CP), de forma vinculada(somente pode ser cometido pelos meios de execução descritos no tipo penal) ou de forma livre (pode ser cometido por qualquer meio de execução), conforme o caso, formal (se consuma sem a produção do



resultado naturalístico, embora ele possa ocorrer), instantâneo (a consumação não se Ciências Humanas e Sociais Unit | Aracaju | v. 2 | n.3 | p. 215-236 | Março 2015 | periodicos.set.edu.br 228 | Cadernos de Graduação prolonga no tempo), monossujeito (pode ser praticado por um único agente), simples (atinge um único bem jurídico, a inviolabilidade da intimidade e da vida privada da vítima) (MAGGIO (2013, [n.p.])).

Esses aspectos se relacionam aos Crimes virtuais que podem ser assinalados em próprios ou puros, bem como, em impróprios ou impuros:

Atos dirigidos contra um sistema de informática, tendo como subespécies atos contra o computador e atos contra os dados ou programas de computador. Atos cometidos por intermédio de um sistema de informática e dentro deles incluídos infrações contra o patrimônio; as infrações contra a liberdade individual e as infrações contra a propriedade imaterial (FERREIRA apud CARNEIRO, 2012, [n.p.]).

Ao considerar os referidos aspectos é importante ressaltar que, a classificação mais apropriada ao contexto atual é a que os crimes podem ser enquadrados como próprios ou impróprios.

7.1 Delitos virtuais próprios

Os crimes virtuais próprios podem ser nomeados em que o sujeito usa um computador, tornando-se o sistema informático do sujeito passivo, aonde o aparelho tecnológico é usado como objeto para o desempenho de certo crime. Destaca-se, que os crimes virtuais próprios invadem dados sem a autorização, por meio de dados catalogados com o uso da informática, salvos em algum aparelho computador, cita-se, a invasão em um sistema com a finalidade de mudar, ou mesmo introduzir dados caluniosos, assim, afetando o software ou o hardware de um computador.

Neste contexto, se insere os crimes virtuais próprios em que o sujeito ativo usa a sistemática da informática do sujeito passivo, na qual o aparelho do computador é empregado como elemento para efetivação do crime.



Nessa categorização de crimes consta, a invasão de dados não permitidos, bem como o intermédio com dados informatizados como, a experiência, da invasão de dados gravados em computador, pode ser no alvo de transformar, induzir, pôr dados caluniosos, ou que abordem o software ou hardware do computador e só podem ser consolidados pelo computador ou contraposição ele e seus periféricos.

Para Viana crimes virtuais próprios: “são aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados)” (VIANA, 2003 apud CARNEIRO, 2012).

Damásio explana sobre os crimes digitais puros ou próprios:

São aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado (DAMÁSIO, 2003).

Deste modo, adentrariam os procedimentos cometidos por hackers, tanto de incursão de sistemas, quanto de colocar informações caluniadoras, que alcancem o software ou hardware do computador só podem ser materializados pelo computador ou seus equipamento físico do computador, bem como, aqueles onde o bem jurídico resguardado pela norma penal é a inviolabilidade de informações, cita-se a interceptação forma ilegal, prevista no artigo 10 da lei 9296/96.

7.2 Delitos virtuais impróprios

Os crimes virtuais designados impróprios são aqueles realizados com o uso do computador, ou outro aparelho digital para consumação de procedimentos ilegítimos abrangendo todo o bem jurídico já tutelado, crimes, deste modo já caracterizado desempenhados com o uso do computador e da internet, utilizando o sistema operacional de informática seus elementos como mais uma ferramenta para efetivação do crime.



Neste sentido, Damásio esclarece que os crimes eletrônicos impuros ou impróprios são:

[...] Aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço "real", ameaçando ou lesando outros bens, não computacionais ou diversos da informática (DAMÁSIO, 2003).

Nesta perspectiva, podemos citar como crimes virtuais impróprios: a calúnia (art. 138 do Código Penal), difamação (art. 139 do Código Penal), injúria (art. 140 do Código Penal), todos estes podem ser perpetrados no campo digital, por meio de um e-mail, bate-papo, dentre outros.

Assim, o que atrapalha a justiça pertinente a punibilidade de tais procedimentos perpetrados pela internet é identificar os sujeitos, pois, a mostra de provas que demonstrem a forma do crime e a acomodação dessa peculiaridade de crime exercido em âmbito virtual com os delitos em natureza já previsto em lei é precária.

7.3 Sujeito ativo

Tendo em vista, ao agente do crime e sua prova difícil devido à ausência física do sujeito ativo (GUBERT, 2023). Em virtude da relevância para comprovar o causador do crime, nasceu à necessidade de se delinear um perfil nomeado grupos que praticam crimes virtuais, dentre essas qualificações temos a figura do hacker.

Conforme a tradução do dicionário Michaelis (2009) hacker significa, “pessoa que usa seu conhecimento técnico para ganhar acesso a sistemas privados”. Assim, a pessoas que detém de conhecimentos inerentes a informática e sistemas usados de seus conhecimentos não apenas para práticas ilícitas, a partir do momento que vislumbra que hackers são pessoas com um vasto conhecimento, é plausível haver conhecimento técnico com formato, tanto positivo, quanto negativo.



Assim sendo, hacker é categoria, enquanto as classes de hackers podem ser variantes conforme as práticas; essa expressão foi inventada na década de 1985, por hackers que não aderiam com o uso do termo hacker pela imprensa para determinar técnicos ou usuários de computadores que cometessem atuações ilegítimas ou que ocasionassem desordem para outras pessoas.

Há duas expressões muito parecidas, são os hackers e os crackers pertinente ao extenso conhecimento em informática, sendo que a principal altivez é a intenção que suas práticas implicam, pois os hackers desempenham atividades positivas, não criminais, enquanto crackers impulsiona o crime em seu cerne, operando, normalmente, com a finalidade delituosa de conseguir proveitos ilegítimos.

Tendo consciência dessa complexidade, citam-se os hackers titulados lamers, de wannabes ou script-kid, estes agem em baixos feitos, restringindo seus conhecimentos e não simulam tanta ameaça, sendo qualificados como leigos diante às amplas maneiras de hackers, pertinentes as espécies incluímos os phreakers que comentem crimes característicos direcionados para o campo de telecomunicações e os defacers que anotam seus indicadores ao dominarem espaços na internet e alterá-las.

Mas nesse jogo de interlocuções, surge a categorização desses perfis de delituosos, assim, imaginemos quem eles são, o que desejam de uma forma geral e como agem, pertinente ao sujeito ativo sabemos que as informações impetradas para identificar o sujeito é o endereço da instrumento que envia as informações, ou seja, o IP, seu login e senha, entretanto com a probabilidade de dissimulação das informações e o uso de dados falaciosos, dificilmente há uma identificação rápida do sujeito ativo na prática.

7.4 Sujeito passivo



Tratando-se dos crimes virtuais, envolvendo uma pessoa física ou jurídica ou um titular incidi em pública ou privada titular do bem jurídico tutelado, consecutivamente haverá o sujeito passivo, alguma pessoa que está sendo lesado, enfim o que experimenta o feito, a vítima.

E em razão dessas situações, o sujeito passivo da infração penal pode ser um indivíduo civil, pessoa física, ou uma pessoa jurídica, em que, pode ter seus bens eliminados, seu patrimônio inutilizado, até mesmo dado infringidos.

Diante de tal concepção é necessário lembrar, que vários dos crimes cometidos ficam no anonimato, isto é, não são noticiadas, talvez pelo desconhecimento das leis que os amparam, em virtude desse desconhecimento por parte de muitas pessoas, elas não denunciam, cita-se: gigantes empresas que poupam a publicação sobre prováveis ofensivas virtuais ou mesmo invasões para não evidenciarem fragilidade pertinente à segurança, já as pessoas físicas observamos que por falta da carecida punição aos transgressores e a ausência de organismos de denúncia, embora já existam, as vítimas preferem não denunciarem o que provoca a difusão desses delitos.

8 AÇÃO PENAL: LEI E CONDUTAS PUNÍVEIS

A ação penal é tida como o direito de buscar o Poder Judiciário, com o intento de apresentar a este a informação do caso de uma infração penal, para que seja aplicado o direito penal objetivo. O assunto encontra-se incluído nos Arts. 24 a 62 do Código de Processo Penal e Arts. 100 a 106 do Código Penal.

Visto que, a Ação Penal é o direito subjetivo público autônomo e abstrato de chamar a tutela jurisdicional do Estado para que este delibere conflitos originários da prática de procedimentos determinadas em lei como crime.



Neste sentido, o “Crime” é a conduta que fere os direitos individuais e sociais do indivíduo e da sociedade. Em virtude disso, é importante destacar os exemplos do doutrinador Avena (2014):

A sua prática gera ao Estado o poder-dever de punir. Como esta punição não pode ser arbitrária nem ocorrer à revelia das garantias INDIVIDUAIS do indivíduo são necessárias a existência de uma fase prévia de apuração, assegurando-se ao possível responsável o direito de defesa, o contraditório e a produção de provas (AVENA, 2014, p. 224).

Em meio às condutas puníveis, eis que surge a Lei nº 12.737/2012 – Lei dos Crimes Cibernéticos, conhecida como a Lei “Caroline Dickmann”, que ocasionou mudanças ao Decreto-Lei 2.848/40 – Código Penal brasileiro, ao formalizar a tipificação de condutas criminosas no campo informático, estabelecendo os “crimes cibernéticos”.

Outra inferência de tal manifestação é a tipificação dos crimes virtuais contida no primeiro artigo do mencionado diploma legal, no entanto, valendo-se da hermenêutica jurídica, aonde se decodifica “crimes informáticos”, devem ser decodificados como “crimes cibernéticos”.

Outro aspecto muito difundido dessa concepção é o segundo do artigo citado, abordando alterações na seção IV do Código Penal brasileiro, que discute dos crimes contra a inviolabilidade dos segredos, assim, acrescentando ao sumário penal os artigos 154-A e 154-B.

Tais considerações apontam que ambos os referidos artigos de Lei buscam resguardar de quaisquer violações pertinentes aos delitos cometidos através dos dispositivos informáticos.

E ainda em relação a essa situação, vale mencionar, os Crimes Cibernéticos, inseridos na Lei nº 12.737/2012, em seu artigo 154-A. *Ipsis litteris*:



Outra inferência de tal manifestação está inserida e no Art. 154-A, referenciando sobre a questão de invadir dispositivo informático de outrem, interligado ou não à rede de computadores, mediante violação imprópria de organismo de segurança e com a finalidade de conseguir, 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.

Acrescenta ainda o artigo Art. 154-A:

§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.

§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:

I - Presidente da República, governadores e prefeitos;

II - Presidente do Supremo Tribunal Federal;

III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembléia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou

IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal (BRASIL, 2012).



O caput do dispositivo acima transcrito (art. 154-A do CP) é considerado o maior avanço harmônico por essa norma, no sentido de amparar as vítimas que usam o mundo virtual.

E ao considerar essa perspectiva, é importante enfatizar que sua finalidade principal é promover o combate às principais práticas prejudiciais, notórias por causarem perturbação para quem se usa ou necessita dessas ferramentas tecnológicas. Os novos artigos inseridos no Código Penal Brasileiro pela Lei 12.737/2012 procuram combater a incursão de aparelhos informáticos de outrem, ligados ou não à rede de computador.

É importante explanar sobre os dispositivos informáticos, sendo assim: o computador de mesa, notebook, laptop, ultrabook, tablete, ipad, smartphone etc. O tipo penal recomenda, além disso, a necessidade de o dispositivo informático ter alguma estrutura de segurança, sob pena de ser analisado desprotegido penalmente (NUCCI, 2013, p. 742).

Ao considerar os referidos aspectos é importante ressaltar que, para perpetrar a conduta tipificada no referido artigo o sujeito ativo precisará submergir, violar/transgredir o dispositivo de outrem, sem precisar ficar interligado com a rede de computadores, e com a finalidade de conseguir, adulterar ou destruir dados ou dados.

Em face disso, o § 1º, cataloga como condutas do modo normativo produzir, oferecer, distribuir, vender ou difundir, compõem métodos que estar sujeito das condutas típicas previstas no caput do artigo 154-A, isto é, para cometer a conduta tipificada neste parágrafo, o sujeito deverá acumular os dados objetivos e subjetivos do tipo.

Enquanto os parágrafos 2º ao 5º do referido artigo, presumem formatos qualificadas pelo efeito, as quais, em resumo, serão assim, caracterizadas se a invasão apresentar como resultado a aquisição de conteúdo de comunicações eletrônicas privadas segredos comerciais



ou industriais ou sigilosos ou controle remoto não permitido do dispositivo atacado, sendo que, nestas pressuposições, a pena será de reclusão de seis meses a dois anos, e multa.

Em decorrência dessa realidade, havendo a exposição, comercialização ou transmitância a terceiros das informações impetrados mediante as citadas condutas delitivas, a pena será acrescentada de um a dois terços. Nesse mesmo sentido, aumenta-se de um terço ou até a metade se o crime perpetrado for cometido contra o Presidente da República, governadores e prefeito, Presidente do STF, o da Câmara dos Deputados e Senador, o da Assembléia Legislativa, o presidente da Câmara Legislativa do Distrito Federal e Municipal e contra pessoas que possuam “cargos máximos” da administração pública direta e indireta, independente da esfera.

Alia-se a esse fato, os crimes contra inviolabilidade dos segredos têm previsão em passagem dessa realidade situacional, advindo da proteção da intimidade e da vida privada da pessoa (BRASIL, 1988, art. 5º, inciso X).

Diante de tal concepção é necessário lembrar, que o art.154 B do CP, traz a identificação da natureza da ação penal, disposto, como regulamento universal aplicativo aos crimes cibernéticos, a ação penal pública condicionada à representação, ou seja, aquela em que a vítima precisará permitir a autoridade policial para desempenhar as averiguações e o membro do Parquet a dar início a a persecução penal.

E ainda em relação a essa situação, vale mencionar que a ação penal será pública incondicionada, isto é, não terá necessidade de representação da vítima, quanto à conduta for cometida em descrédito da administração pública direta ou indireta em qualquer campo da União.

Dentro desse contexto, teceremos algumas pontuações acerca do terceiro artigo da citada lei, o qual modificou a redação do art. 266 do CP, compreendendo à forma do tipo



normativo o serviço informático, telemático ou de informação de utilidade pública, presumindo, apesar, que a interrupção ou perturbação das novas formas de comunicação é crime (OLIVEIRA, 2013). Assim, o legislador pátrio ponderou bem no momento dessa atualização, fazendo necessária devido às novas transformações da “era cibernética”.

Tais elementos o são permeiam a modalidade: interromper, perturbar, impedir ou dificultar, isto é, o sujeito será incapaz de executar, obstar ou romper o serviço, não havendo, até mesmo, elementos subjetivos de tipo específico (OLIVEIRA, 2023). Já às formas qualificadas pelo resultado, assim analisada quando o crime for cometido em época de catástrofe pública, a pena a ser aplicada será em dobro.

Já no artigo 298 do CP acrescentou o parágrafo único, o qual desempenhou a comparando o cartão de crédito e de débito com documentos particulares (COSTA, 2012).

Enquanto o quarto artigo da Lei “Carolina Dickman” apresenta alinhamentos acerca da vacatio legis, a norma entraria em vigor em 120 (cento e vinte) dias após a sua publicação oficial.

9 INEFICIÊNCIA NAS LEIS BRASILEIRAS

Este capítulo aborda a impunidade no nosso país, onde as leis quase sempre não são aplicadas de forma correta. Incide que o sistema criminal apresenta de maneira falha, além de ser mal aplicadas pelo judiciário permeia a demora, assim, contribuindo com a impunidade no nosso país.

Ainda que seja bastante crítica essa visão conota que esses criminosos cibernéticos, ainda arrumam uma maneira de driblar a justiça com as lacunas que há na mesma, isso fortalece esse mundo delituoso em que os citados se utilizam de parte dos remédios constitucionais para se beneficiar, bem como recursos. Dessa forma, esses criminosos



ganham espaço ara continuarem cometendo práticas delituosas, comprometendo a imagem de muitas pessoas.

Tendo consciência dessa complexidade, diante o Direito Penal e o Sistema Criminal Brasileiro. Entendemos que a aplicação das leis, com tanta demora na aplicação, bem como a impunidade no nosso país, gera fragilidade no caso dos delitos virtuais.

E em razão dessas situações, diariamente somos informados de fatos que abrangem crimes virtuais graves e que muito destes crimes são de encomendados aos especialistas na área da virtual, estes agem na certeza da impunidade, pois, já conhece o sistema criminal brasileiro, aliado a isso, há a dificuldade de identificar os criminosos, pois, ainda não há celeridade na descoberta dos crimes cibernéticos.

Tais considerações apontam que percebemos a necessidade do poder judiciário cumpra o seu papel de maneira célere com as leis, sem deixar brechas para que se possam driblar as leis e ficar impune os delituosos dos crimes que cometem.

Diante de tal concepção é necessário lembrar que o cenário contemporâneo, muitos estar sujeito de mecanismos eletrônicos para armazenamento de informações, sejam indicativos à vida íntima ou profissional. Pois, os aparelhos de proteção aos recursos computacionais não são adequados em sua integralidade. Desta forma, é indispensável meios dinâmicos para avalizar a proteção e segurança dos indivíduos, que devem gozar de sua intimidade e vida privada, tal como assegura a Constituição Federal de 1988 em seu Artº 5º, V.

5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação (BRASIL, 1988).



No Brasil, são vários os casos de publicação de conteúdo sem autorização das pessoas, e que sucedem meio de incursão computacional. Pesquisas assinalam que as mulheres são vítimas periódicas de tal procedimento, segundo a Safernet Brasil, em 2016, 300 pessoas tiveram suas fotos íntimas vazadas. Destas, 202 eram mulheres.

Ainda que seja bastante crítica essa visão conota que há ocasiões em que casais trocam fotos, fotos sem vestimentas, por sentir segurança em seu parceiro, mas que a conclusão de relacionamento, como forma de represália ou de não consentimento, um deles apronta por noticiar o conteúdo, que pode ocasionar danos irreparáveis à pessoa revelada.

É bom lembrar que embora haja tipificação para tal conduta, as punições não são satisfatórias para reduzir os criminosos. Um indivíduo dissemina as fotos, ele perpetra o crime, entretanto quem sofre as maiores consequências é a pessoa exposta.

Um ponto que cabe a ser destacado é que os crimes que cometidos com maior assiduidade em no Brasil são: crimes contra a honra, divulgação de fotos sem autorização e a pedofilia e pornografia infantil. Os culpados pelo cometimento de tais delitos não são culpados a magnitude de suas condutas. Os sujeitos passivos lidam consequências que vão além do campo virtual, várias vezes, abrangem a vida íntima e ocasionam decorrências que poderão persistir por um longo período.

Em razão dessa realidade o Código Penal brasileiro tipifica outras performances que se emolduram ao ambiente web, entretanto, tem penas afáveis e não suficientes para coibir a prática destes atos. A lei Carolina Dickman (Lei 12.737/2012), mencionada anteriormente alterou o Código Penal e introduziu artigos em seu conteúdo, contudo, a despeito de explicitar procedimentos praticados na web, apresenta duvidosas explicações e penalidades serenas aos criminosos. Assim, a falta de uma legislação característica ao *cybercrime*, ativa a ideia de que na internet tudo pode.



Ao considerar os referidos aspectos é importante ressaltar que, é preciso a produção de uma legislação que aborde sobre crimes cometidos no ambiente virtual, visto que, são comuns e apresentam a suas vítimas prejuízos reais. A penalidade proporcional é uma forma de controlar a prática destes crimes, pois poderá replicar de forma penosa, o cracker.

Ao levar em consideração esta perspectiva, é importante situar, sabendo dos resultados ocorridos dos crimes cibernéticos, deve-se instituir uma lei que não mais admita que a internet, melhor e mais ágil forma de comunicação/interação virtual, seja utilizada de forma maléfica aos seus usuários.

10 CONCLUSÃO

Neste trabalho abordamos a história da internet e a sua difusão mundial, bem como a necessidade do direito em atualizar as alterações incididas em razão da nova comunidade tecnológica provocada pelo progresso da informática. Embora haja uma legislação atuante, mas é insuficiente para a distinção dos delitos virtuais, a publicação da Lei n. 12.737/2012 estabeleceu um importante avanço, ao tipificar o delito de “invadir dispositivo informático”, indicando um tipo penal que apontou de modo notável resguardar o sigilo de dado e informação pessoal ou profissional.

Dessa forma, avaliamos os elementos típicos básicos do crime: criminalidade na rede, categorização doutrinária dos crimes cibernéticos, delito virtual próprio, delito virtual impróprio, sujeito ativo e passivo, ação penal e a apuração dos delitos informáticos, lei e condutas puníveis. Trata-se de um assunto complexo, atual e que deverá permanecer como um instigante campo de pesquisa para os próximos estudos.

Cumprimos com todos os objetivos que tínhamos proposto ao permear a produção da pesquisa, que se iniciou com estudos teóricos, chegando até a análise a partir dos casos de crimes apresentados em trabalhos já publicados. A partir desse trabalho observei aspectos



importantes no intuito de mencionar meus atendimentos finais sobre a temática em questão. Para isso, tomo como referências as temáticas que surgiram dos depoimentos dos professores participantes da pesquisa.

Vivemos atualmente inúmeras transformações, os avanços do mundo globalizado têm feito a sociedade contemporânea caminhar em uma direção que tem favorecido tanta positiva, quanto o negativo. Isso para as pessoas que buscam a internet em meio às mídias sociais vinculadas ao uso das tecnologias, ferramenta que também beneficia a formação pessoal, avanços no cenário dos negócios, devendo assumir uma postura mais ativa na constituição do seu próprio saber e analisa como uma opção viável em busca de resguardar essas categorias.

Ainda sobre esse texto demonstramos fatos relacionados aos crimes cibernéticos ou cybercrimes. Tendo por finalidade apresentar a insuficiência de tipificações com cunho de punir crimes virtuais, analisar o uso das mídias sociais nos crimes digitais, bem como, contextualizar a historicidade da internet, avaliar a ação penal e a apuração dos delitos informáticos.

E ainda em relação a essa situação, vale mencionar a demora jurídica faz com que pessoas com mau caráter, com conhecimentos aprofundados na arte de programação os designados crackers, passam a produzir ações de cunho maléfico, nas modalidades de crimes contra a honra, divulgação de informações pessoais.

E em razão dessas situações os resultados mostraram necessidades, a ideia de leis rigorosas se faz necessária para a erradicação destes delitos, pois os agentes ocasionadores do delituoso deixam de ser responsabilizados dos prejuízos causados.

E ao considerar essa perspectiva, é importante enfatizar que diante a divulgação, unificados a mensuração das poucas leis atuais e aplicadas, o trabalho, espera uma expectativa de questões ligadas aos ilegítimos realizados por intermédio da Internet com as leis vigorantes.

Este trabalho foi muito importante para meu crescimento, tanto pessoal, quanto acadêmico, provocando-me, a compreensão, bem como o aprofundamento deste tema, pois,



permitiu-me conhecer melhor o desdobramento do fenômeno, além de ter-me permitido aperfeiçoar competência pertinente a investigação.

REFERÊNCIAS

AVENA, Noberto Cláudio Pancaro. Processo Penal: esquematizado/ Noberto Avena- 2. Ed. –Rio de Janeiro: Forense; São Paulo: Método, 2010, p. 230.

BRASIL. Lei n. 12.737, de 30/11/2012. http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/112737.htm. Acesso em: 29 OUT. 2019.

_____. Constituição da república federativa do Brasil de 1988. Brasília: Palácio do Planalto. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm . Acesso em: 21 OUT. 2019.

CARNEIRO, Adenele Garcia. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. Âmbito Jurídico, Rio Grande, XV, n.99, abr. 2012. Disponível em: <https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-para-uma-reflexao-sobre-o-problema-na-tipificacao/>. Acesso em: 22 out. 2019.

DAMÁSIO DE JESUS, E. De. **Direito penal: geral**. 23. ed. São Paulo: Saraiva, 1999.

DULLIUS, Aladio Anastácio. Dos crimes praticados em ambientes virtuais. 2012. Disponível em: <http://www.conteudojuridico.com.br/consulta/Artigos/30441/dos-crimes-praticados-em-ambientes-virtuais>. Acesso em: 29 out. 2019.

EDWARDS, Paul N., 1996. The Closed World. Cambridge, MA, MIT Press.

GOUVEIA, Sandra Medeiros Proença. O direito na era digital: Crimes praticados por meio da informática. Rio de Janeiro: Mauad, 1997.

GUERRA, A. de L. e R. METODOLOGIA DA PESQUISA CIENTÍFICA E ACADÊMICA. **Revista OWL (OWL Journal)**, [S. l.], v. 1, n. 2, p. 149–159, 2023. DOI: 10.5281/zenodo.8240361. Disponível em: <https://www.revistaowl.com.br/index.php/owl/article/view/48>. Acesso em: 17 set. 2023.

HAFNER, K. Lyon, M., 1996, Where wizards stay up late: the origins of the Internet. New York, Simon & Schuster.



REVISTA OWL (*OWL Journal*)

www.revistaowl.com.br – ISSN: 2965-2634

MAGGIO, Vicente de Paula Rodrigues. Novo crime: invasão de dispositivo informático - CP, Art. 154-A. Disponível em: <https://vicentemaggio.jusbrasil.com.br/artigos/121942478/novo-crime-invasao-de-dispositivo-informatico-cp-art-154-a>. Acesso em: 17 out. 2019.

MICHAELIS. <https://michaelis.uol.com.br/>. Acesso em: 29 out. 2019.

MARTINS, Elaine. O que é world wide web? 2008. Disponível em: <https://www.tecmundo.com.br/web/759-o-que-e-world-wide-web-.htm>. Acesso em: 12 out. 2019.

MERKLE, E. R.; RICHARDSON, R. Digital dating and virtual relating: conceptualizing computer mediated romantic relationships. Ohio: Family Relations, Kent State University, 2000.

MIRANDA, Marcelo Baeta Neves. Abordagem dinâmica aos crimes via internet. Disponível em: <https://jus.com.br/artigos/1828/abordagem-dinamica-aos-crimes-via-internet/2>. Acesso em: 29 out. 2019.

MORAN, J. M. Novos caminhos do ensino à distância. Informe CEAD - Centro de Educação à Distância. SENAI. Rio de Janeiro, Ano 1, n. 5, out/nov/dez 1994.

MONTEIRO, J; SILVA, D. História da Internet. 2009. Disponível em: <<http://pt.slideshare.net/guest06f3c/historia-da-internet-1162354>>. Acesso em: 22 out. 2019.

NUCCI, Guilherme de Souza. Código penal comentado: estudo integrado com processo e execução penal. 14. ed. Rio de Janeiro: Forense, 2014.

OLIVEIRA, A. A ILEGALIDADE DO CANCELAMENTO DE PLANOS DE SAÚDE SEM COMUNICAÇÃO PRÉVIA: UMA ANÁLISE JURÍDICA E ÉTICA. **Revista OWL (OWL Journal)**, [S. l.], v. 1, n. 1, p. 113–123, 2023. DOI: 10.5281/zenodo.7955408. Disponível em: <https://www.revistaowl.com.br/index.php/owl/article/view/17>. Acesso em: 17 set. 2023.

OLIVEIRA JÚNIOR, E. Q. de. A nova Lei Carolina Dieckmann. Disponível em: https://www.migalhas.com.br/dePeso/16,MI169227,21048_-A+nova+lei+Carolina+Dieckmann. Acesso em: 17 out. 2019.

PASSOS, José Joaquim Calmon de. **Direito, poder, justiça e processo? Julgando os que nos julgam**. Rio de Janeiro: Forense, 2003.

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-> <www.mail.google.com>. Acesso em: 17 out. 2019.



REVISTA OWL (*OWL Journal*)

www.revistaowl.com.br – ISSN: 2965-2634

ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2004

ROSA, Fabrizio. Crimes de Informática. Campinas: Bookseller, 2002.

ROQUE, Sérgio Roque. Criminalidade Informática – Crimes e Criminosos do Computador. 1 ed. São Paulo: ADPESP Cultural, 2007.

SILVA, Rita de Cássia Lopes da. Direito penal e sistema informático. São Paulo: Revista dos Tribunais, 2003.

SCHMIDT, Guilherme. Crimes cibernéticos. Jusbrasil, 2014. Disponível em: < <http://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos>>. Acesso em: 12 out. 2019.

TERCEIRO, Cecilio da Fonseca Vieira Ramalho. **O problema na tipificação penal dos crimes virtuais**. Disponível em: <<http://jus.uol.com.br/revista/texto/3186/o-problema-na-tipificacao-penal-dos-crimes-virtuais>>. Acesso em: 29 out. 2019.

VALZACCHI, Jorge R. Internet y educacion: aprendiendo y ensensando em los espacios virtuales. 2ª ed. Versão Digital, 2003. Disponível em: . Acesso em: 12 out. 2019.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. Crimes cibernéticos: ameaças e procedimentos de investigação. 2ª Ed. Rio de Janeiro: Brasport, 2013.

WILLIAM THOMAS GUBERT. SUSPENSÃO PROCESSUAL NO ÂMBITO DAS AUDIÊNCIAS TRABALHISTAS DURANTE A PANDEMIA DA COVID-19. **Revista OWL (OWL Journal)**, [S. l.], v. 1, n. 1, p. 230–239, 2023. DOI: 10.5281/zenodo.7996739. Disponível em: <https://www.revistaowl.com.br/index.php/owl/article/view/28>. Acesso em: 17 set. 2023.

Recebido em: 07/09/2023

Aprovado em: 13/09/2023

Publicado em: 17/09/2023