PEDRO HENRIQUE CIQUEIRA GUIMARÃES

EVOLUÇÕES DOS CRIMES VIRTUAIS E SEUS IMPACTOS NA SOCIEDADE:

CUIABÁ/MT
2022

PEDRO HENRIQUE CIQUEIRA GUIMARÃES

EVOLUÇÕES DOS CRIMES VIRTUAIS E SEUS IMPACTOS NA SOCIEDADE:

Trabalho de Conclusão de Curso apresentado à Faculdade UNIC de Cuiabá - MT como requisito parcial para a obtenção do título de graduado em Direito.

Orientador(a): Carina Kamei

CUIABÁ/MT
2022

PEDRO HENRIQUE CIQUEIRA GUIMARÃES

EVOLUÇÕES DOS CRIMES VIRTUAIS E SEUS IMAPACTOS NA SOCIEDADE:

Trabalho de Conclusão de Curso apresentado à Faculdade UNIC de Cuiabá - MT como requisito parcial para a obtenção do título de graduado em Direito.

BANCA EXAMINADORA

Prof(a). Titulação Nome do Professor(a)

Prof(a). Titulação Nome do Professor(a)

Prof(a). Titulação Nome do Professor(a)

Cuiabá/MT, 06 de dezembro de 2022.

Dedico este trabalho aos meus colegas de curso, que assim como eu encerram uma difícil etapa da vida acadêmica.

AGRADECIMENTOS

Em primeiro lugar, a Deus, no qual fez com que meus objetivos fossem alcançados, durante todos os meus anos de estudos. A todos que participaram, direta ou indiretamente do desenvolvimento deste trabalho de pesquisa, enriquecendo o meu processo de aprendizado. À instituição de ensino UNIC, essencial no meu processo de formação profissional, pela dedicação, e por tudo o que aprendi ao longo dos anos do curso.

Quando vou a um país, não examino se há boa leis, mas se as que lá existem são executadas, pois, boas leis hão por toda a parte.

(Montesquieu)

CIQUEIRA GUIMARÃES, Pedro Henrique. **Evoluções dos crimes virtuais e seus impactos na sociedade.** 2022. 34. Trabalho de Conclusão de Curso (Graduação em Direito) – Universidade de Cuiabá, Cuiabá, 2022.

RESUMO

Este estudo objetivou compreender o Estudo dos delitos Cometidos em âmbito especificamente virtual e entender as principais dificuldades encontradas pelos operadores do Direito no momento de determinar autoria e assim punir os infratores. sendo de suma importância este assunto que se justifica pela grande dificuldade de punir os infratores de crimes cibernéticos, e enfatizando o aumento crescente de crimes nesta modalidade em nosso país, fazendo-se apontamentos pela falta de legislação específica, tornando-se assim um grave problema jurídico e social. Diante disto, analisamos o presente feito de forma minuciosa visando entender deste os breves momentos históricos do relacionamento entre o direito a informática e o surgimento de crimes que se originaram neste campo virtual até os dias atuais. sabe-se que a situação atual do Brasil em relação ao aumento deste tipo de crime é alarmante levando em consideração o alto índice de delitos cometidos, pois com a globalização e os efeitos do período de Pandemia em que o Mundo passou, ferramentas virtuais passaram a ser mais do que uma ferramenta de pesquisa e entretenimento social, sendo assim uma ferramenta de trabalho e de meio de subsistência moderna.

Palavras-chave: Crimes Cibernéticos. Cibercrimes. Crimes. Delitos. Internet. Crakers. Hackers.

CIQUEIRA GUIMARÃES, Pedro Henrique**. Evolutions of virtual crimes and their impacts on society.** 2022. 34. Course Completion Work (Graduate in Law) – University of Cuiabá, Cuiabá, 2022.

ABSTRACT

This study aimed to understand the Study of Crimes Committed in a specifically virtual environment and to understand the main difficulties encountered by legal operators when determining authorship and thus punishing offenders. being of paramount importance this subject that is justified by the great difficulty of punishing the offenders of cyber crimes, and emphasizing the growing increase of crimes in this modality in our country, making notes for the lack of specific legislation, thus becoming a serious problem legal and social. In view of this, we analyze the present made in a detailed way in order to understand the brief historical moments of the relationship between the right to information technology and the emergence of crimes that originated in this virtual field until the present day. It is known that the current situation in Brazil in relation to the increase of this type of crime is alarming, taking into account the high rate of crimes committed, because with globalization and the effects of the Pandemic period in which the World passed, virtual tools began to be more than a tool for research and social entertainment, it is therefore a tool for work and modern livelihood.

Keywords**:** Cyber Crimes. cybercrimes. crimes. offenses. Internet. Crackers. Hackers.

LISTA DE ABREVIATURAS E SIGLAS

EDV-Recht	Elektronishen Datenverarbeitung Recht
MPF	Ministério Público Federal
ONU	Organização das Nações Unidas
PLC	Projeto de Lei da Câmara
PL	Projeto de Lei
STJ	Superior Tribunal de Justiça

SUMÁRIO

1 INTRODUÇÃO

O Estudo do Direito acompanha a evolução da sociedade a qual encontra principalmente na área cibernético, formas de atuação ou inserção de seus mecanismos de funcionamento. Através da internet, que hoje em dia é considerada o principal meio de trocas de informações da sociedade, o Direito encontra a possibilidade de oferecer segurança às várias e diversas relações jurídicas e procura, podendo-se dizer que a passos largos, transitar cada vez mais entre o mundo real e o virtual. Todavia certas informações digitais podem conferir instabilidade e lesividade as relações consideradas, visando o fácil acesso ao mundo digital por grande parte da população que usa.

Crime cibernético é uma atividade criminosa que tem como alvo ou faz uso de um computador, uma rede de computadores ou um dispositivo conectado em rede. Não todos, mas a maioria dos crimes cibernéticos é cometida por cibercriminosos ou hackers que querem ganhar dinheiro ou obter vantagens diversas. O crime cibernético é realizado por pessoas ou organizações. Raramente o crime cibernético visa danificar os computadores por outros motivos que não o lucro. Nesses casos, os motivos podem ser pessoais ou políticos.

A presente pesquisa que tem como tema “Evoluções dos crimes virtuais e seus impactos na sociedade”, sendo importante este assunto se justificando pela grande dificuldade de punir os infratores de crimes cibernéticos enfatizando o aumento crescente de crimes desta modalidade em nosso país, e pela falta de legislação específica tornando-se assim um grave problema jurídico e social. Diante disto, analisando de forma minuciosa sabe-se que a situação atual do Brasil em relação ao aumento deste tipo de crime é alarmante levando em consideração o alto índice de delitos cometidos, pois com a globalização e os efeitos do período de Pandemia em que o Mundo passou, ferramentas virtuais passaram a ser mais do que uma ferramenta de pesquisa e entretenimento social, sendo assim uma ferramenta de trabalho e de meio de subsistência moderna.

Isso mudou totalmente o nosso conceito de espaço físico e fronteiras comerciais e de geração de Renda. Logo Inevitavelmente, houve a migração de vários criminosos para este mundo, com intuito de tirar proveito ou coisa diversa por meios ardilosos. Contudo através de estudos e análises através de índices, mostra-se o

aumento dos crimes virtuais e da preocupação da população. Valendo Ressalva de que que a norma jurídica não evoluiu na mesma proporção dos crimes virtuais, a cada dia surgem novos tipos penais e o estado não pode punir os infratores por ausência de leis específicas.

Crime cibernético é uma atividade criminosa que tem como alvo ou faz uso de um computador, uma rede de computadores ou um dispositivo conectado em rede. Não todos, mas a maioria dos crimes cibernéticos é cometida por cibercriminosos ou hackers que querem ganhar dinheiro ou obter vantagens diversas. Assim a seguinte pesquisa visa responder ao seguinte questionamento: Quais são as principais dificuldades encontradas pelos operadores do direito no que diz respeito a punir os infratores?

Temos como Objetivo Geral: entender as principais dificuldades encontradas pelos operadores do Direito no momento de determinar autoria e assim punir os infratores. Para alcançarmos esse Objetivo geral, temos os objetivos específicos: Relação do Direito e a Informática; principais crimes cibernéticos que são atípicos em decorrência de ausência de lei específica; aplicabilidade dos princípios da legalidade, reserva legal e analogias aos crimes cibernéticos.

O tipo de metodologia a ser realizado neste trabalho, é uma revisão de literatura, por meio do método de pesquisa bibliográfico. Serão realizadas consultas em livros e revistas que abordam o tema, bem como trabalhos científicos como dissertações, teses artigos publicados nos Últimos 15 anos. Serão utilizadas bases de dados e/ou repositórios como o Google acadêmico e a Scielo, para tanto as palavras-chaves utilizadas nas pesquisas serão: crimes virtuais; direito e informática; cibercrimes. O tipo de pesquisa a ser realizada é a pesquisa bibliográfica, com caráter qualitativo e descritivo. Serão apreciados livros, trabalhos científicos e acadêmicos, tanto no formato físico quanto no formato digital, selecionados por meio de buscas relacionadas ao tema da pesquisa.

As pesquisas em meios digitais serão realizadas em repositório públicos como o Google acadêmico e a Scielo, para tanto serão utilizadas as seguintes palavras-chaves: crimes virtuais; direito e informática; cibercrimes. Serão selecionadas as publicações desenvolvidas nos últimos 15 anos. Dada a relevância da pesquisa alguns autores renomados fazem parte desse contexto, em prol desta futura pesquisa alguns autores serão apreciados e reflexões de seus estudos serão realizados. Dentre

esses autores destacam-se: (GONÇALVES, 2015), Higor Vinicius Nogueira Jorge (2012), Pinheiro (2013, apud FERREIRA, 2001), (OLIVEIRA, p.32,2012).

2 DIREITO E A INFORMÁTICA

A Informática é um neologismo derivado do francês informatique, o qual resulta da conjugação de information e automatique. Que tem como significado o tratamento automático ou automatizado de informação. Predominantemente sinônimo de computação, termo mais próximo do inglês computing ou computer sciences. Em alemão utiliza-se a terminologia EDV-Recht (Elektronishen Datenverarbeitung Recht), Computerrecht. Embora sendo muito comum também se utilizar a denominação Direito das Tecnologias da Informação ou Direito da Sociedade da Informação, porém, em outros países latinos como Espanha e Itália, prevalece a designação Direito da Informática. Buscando se adentrar um pouco mais na história, o autor Alessandro Baratta cita em seu livro intitulado como “Criminologia crítica e crítica do direito penal introdução à sociologia do direito penal.” O seguinte marco histórico que se deu origem e início aos primeiros resquícios da Internet.

Para Baratta (2002) “sabe-se que a Internet teve seu marco inicial em plena guerra fria, sendo foi utilizada como uma espécie de arma norte-americana de informação militar. Possuía como a principal função interligar todas as centrais de computadores dos postos de comando táticos, resultando com que os americanos, se prevenissem de uma suposta atividade surpresa de ofensiva russa. Porém se ocorresse algum imprevisto em um desses pontos estratégicos e os americanos fossem atacados, os demais pontos continuariam funcionando de forma autônoma, auxiliando e fornecendo informações a outros centros militares”.

Em dias atuais tem se notado que a Internet interliga milhões de computadores e também dispositivos móveis e não móveis das mais diversas categorias, e sendo mesma, se tornou um “conglomerado de redes” contribuindo assim, para o acesso a todo tipo de informação e transferência de dados. Todavia com o aparecimento da internet e o avanço diário da tecnologia, a população não se tem convivido apenas de benefícios advindas, passou-se a surgir então, junto com os benefícios da internet os crimes cibernéticos e não o bastante, várias vítimas associadas a esses crimes.

O Direito é como uma ciência dinâmica que, tem a capacidade de se modificar e se ajustar à realidade da sociedade, permitindo-se aplicar a norma abstrata à época vivida por ela de forma prudente e justa de forma harmônica. Em tempos modernos, com os avanços da tecnologia da informação e com a chegada da internet, foi criado

um novo cenário jurídico, de escala global, cujo o objeto são as relações interpessoais pelo meio eletrônico, que por sua vez, engloba-se a necessidade da elaboração de normas e regras das quais possam possibilitar sua correta e adequada utilização e manuseio, e disto, cabe ao campo do Direito regular as relações sociojurídicas surgidas da devida influência da informática e da telemática na vida dos indivíduos de uma forma geral.

O Direito da Informática é uma disciplina que busca estudar as implicações e os problemas jurídicos surgidos com a utilização das modernas tecnologias da informação. Com o passar do Tempo está disciplina vem ganhando seu espaço e se consolidando como um novo ramo das ciências jurídicas que sobretudo se completa pela interdisciplinaridade e pela complementaridade, que por sua vez objetiva servir de complemento aos conhecimentos e resultados obtidos nas unidades curriculares tradicionais. A Interdisciplinaridade se molda na medida em que o estudo do Direito da Informática exige, para além do conhecimento de noções básicas de tecnologias da informação. (Lesmes Serrano, 1997)

Apesar de diversos benefícios sociais que a influência da informática trouxe, para os meios de comunicação, sociais e comerciais, por sua vez, em sentindo contrário, a internet também tem sido comumente utilizada como ferramenta para prática de crimes e delitos de diversas naturezas frequentemente encontradas na sociedade, de acordo com o STJ, no ano de 2008 já existiam mais de 17 mil decisões judiciais envolvendo crimes virtuais como estelionato, calúnia, ameaça, bullying, preconceitos contra grupos e etnias e muitos outros. Em 2002 eram apenas 400, o que impulsiona o surgimento da necessidade de adaptação de normas em vigor visando regular as relações neste ambiente. É de fácil percepção a preocupação da comunidade jurídica internacional em elaborar e desenvolver mecanismos de soluções de problemas de origem das relações eletrônicas podendo ser, como, meio utilizado pelo agente causador do crime ou agressão. Neste sentindo vem desabrochando um novo campo do direito que objetiva regular as relações interpessoais e extra pessoais do ambiente virtual ou eletrônico, com a função de designar, conceituar, ou autuar indivíduos delitivos que fazem uso de ferramentas virtuais ou eletrônicas para transgredir, ou tirar proveito de direito alheio ou vantagem ilícita utilizando de artifícios como softwares e hardwares criados e desenvolvidos com finalidade a ser ferramentas de atuação de crimes e delitos. (COÊLHO, 2001)

Na União Europeia, no ano 2001, foi criada a convenção sobre os Cibercrimes (Convenção de Budapeste), que mais de 40 países faziam parte. De forma resumida, a Convenção teria como um dos objetivos tipificar as condutas criminosas, e cria normas de investigação que se dispõe de métodos de cooperação internacional, contudo, no Brasil, por se tratar de uma matéria relativamente nova para o ano em questão, os legisladores se abstiveram quanto ao tema. Porém existiam alguns projetos de lei que tramitam há alguns anos no congresso nacional, como por exemplo o PLC 89/2003, conhecido como Projeto de Lei dos Crimes Eletrônicos. Consequentemente os tribunais ficavam limitados de acordo com o que se aplica o Código Penal Brasileiro sobre o combate destas atividades criminosas. (DELGADO, 2007) Sendo como Objetivo Central, o grande desafio de combater os crimes e delitos cibernéticos e a sua internacionalização. Ou seja, o criminoso não fica limitado a um espaço geográfico ou fronteiras para atuar. Um indivíduo em um país A pode ter a capacidade de realizar atos ilícitos em um país B. acarretando uma enorme dificuldade para ser localizado, e sem uma correta colaboração entre estes países o indivíduo delituoso conseguirá facilmente sair impune de seu ato. Portanto já se destaca o primeiro problema. O ato deve ser considerado ilícito nos dois países. Se em algum deles não tivermos a tipificação jurídica não existe crime, logo, as autoridades daquele país não irão colaborar. Outra dificuldade na colaboração está no processo penal de cada entidade governamental. Como tratar a investigação, a coleta de evidências, cadeia de custódia entre outros fatores que possam ser usados de forma coerente numa investigação internacional. (MPF 2ª, 2014, rev.)

Segundo um dos acadêmicos mais respeitados se tratando de temas relacionadas ao Direito e a Informática, o Professor LAWRENCE LESSIG (1999) “De fato, a web, desde o seu início, sempre foi vista como uma espécie de “terra sem lei”, em que as liberdades individuais devem prevalecer em detrimento de qualquer tentativa de controle externo.” Os inúmeros problemas que surgem nesse contexto anárquico, podendo se destacar toda modalidade de crimes praticados sob a esfera do anonimato, compelem ao Estado elaborar mecanismos regulatórios do âmbito cibernético para impor alguma ordem ao caos que ameaçava se instalar. De maneira paralela, o Estado se viu na eminência de se utilizar de novas ferramentas para realizar, com maior eficiência e eficácia, os seus fins, passando, deste modo, a

suportar das diversas consequências da ausência de legislação específica no universo virtual.

Cabe salientar a fins de complementação de entendimento que, na esfera do Direito Privado temos ações Virtuais comumente produzidas por diversas pessoas, que deliberadamente acabam sendo alvos desses indivíduos delituoso que buscam levar para si ou para outrem vantagem ilícita e criminosa, como por exemplos, os contratos informáticos, e a questão dos nomes de domínio (Domain Name) que são ações que afetam o Direito Civil e Comercial e os crimes ou delitos chamados "informáticos" sendo estes os quais afetam o Direito Penal. Sobre a influência do Direito Informático nos demais ramos do Direito, trazemos à luz a doutrina de Carlos Barriuso Ruiz. (1996) Segundo este autor, o Direito Informático:

> “afecta en mayor o menor medida a todas las demás ramas del derecho entre las que destacamos: la filosofia del derecho, como responsable de fundamentar este nuevo hecho y coordinar las distintas partes implicadas; la socio-laboral, en cuanto que la implantación de las nuevas tecnologías modifica las actuales condiciones de trabajo y emplo, permitiendo relaciones de trabajo nuevas, como el teletrabajo; la mercantil, con las nuevas formas de mercado y contratación; la procesal, definiendo y valorando las pruebas efectuadas por medios electrónicos – informáticos y estableciendo procesos adecuados a la realidad informática; la penal, con el cometido de tipificar y sancionar las nuevas acciones y conductas delictivas que surgen; la administrativa, estableciendo procedimientos más ágiles.” (Barriuso,1996, 1ª e.d).

Sobre a luz da interpretação do Renomado Autor, a adequação de fundamentos e filosofias voltadas a esse âmbito do Direito, deve esta harmonicamente sendo alteradas e modificadas conforme a implementação de novas tecnologias que se modificam de tempos em tempos, visando estabelecer procedimentos adequados e de coerência a tipificar e sancionar novas ações e condutas delitivas que surgem, tornando-se assim, para os profissionais do Direito ferramentas mais ágeis para exercer atividades de investigação e punição destes infratores.

Outra evidente dificuldade na colaboração da aplicação de regulações em âmbito Internacional está no processo penal de cada entidade governamental, Como se deve tratar a investigação, a coleta de provas e evidências, a cadeia de custódia entre outros elementos que possam ser usados de forma coerente em uma investigação internacional. Vale-se citar, que O ato deve ser considerado ilícito nos dois países, por exemplo, se em algum deles não tivermos a devida regulamentação jurídica não existe crime, sendo assim, as autoridades daquele país não vão ter legitimidade para a colaboração nos atos de investigação destes indivíduos.

(PAESANI, 2006). Com o percebimento de toda esta dificuldade, em 23 de novembro de 2001, os países membros do Conselho da Europa, criaram um tratado internacional que promove a cooperação entre os países contra o crime cibernético. Sendo ele o primeiro tratado internacional contra crimes cibernéticos. Já em junho de 2021, 66 países já tinham aderido à Convenção e estima-se que seus artigos produzidos seriam usados como orientação legal em mais de 158 países.

Voltando para o Brasil, este que por sua vez, já se consolidava com algumas Leis que cobrem o cibercrime, sendo as mais famosas o Marco Civil da Internet (Lei 12.965/14) e a Lei Carolina Dieckmann (Lei 12.737/12). Porém muitos atos ilícitos ocorrem sem uma cobertura específica legal e volta e meia, necessitam, de serem reanalisados sobre uma ótica penal similar a evolução do âmbito virtual, aplicativos e tecnologias. Mas nem sempre isto se é possível. Como por exemplo o delito de furto de cartão de crédito ou débito. O cartão virtual não é contemplado em nenhuma legislação. Ou seja, se um criminoso se utilizar de meios ardilosos e conseguir acesso ao cartão virtual da vítima ela não terá como solicitar qualquer espécie de reparo específico a esta modalidade de crime, nem terá amparo legal, uma vez que o cartão virtual não é objeto jurídico. Além de problemas de cooperação internacional que, apesar de vários tratados internacionais do Brasil com outras nações, se vê carecendo de mais atenção. Não obstante a isto, apesar de existirem normas jurídicas que tipificam os crimes cibernéticos, elas acabam não sendo suficientes para abranger os crimes que são cometidos de forma virtual. Assim, dificultando para os investigadores e para os operadores do direito exercerem a atividade punitiva os infratores, devido ao caso de se tratar de um tipo penal, sendo que no direito penal tem que ser respeitado e levado em consideração o princípio da reserva legal, da legalidade penal, não podendo ser aplicado o princípio da analogia. (CARDOSO, 2016)

No Ordenamento jurídico Brasileiro existem hoje duas leis que regulamenta os crimes virtuais. Sendo a mais antiga a lei ordinária 12.735/2012 e a lei 12.737/2012, que ficou conhecida nacionalmente como “Lei Carolina Dieckman”, esta que foi criada após o vazamento de fotos pessoais da atriz Carolina Dieckman, do seu computador pessoal. Apesar de existirem essas duas Leis específicas no que se refere a cibercrimes, devemos ter reconhecimento de que elas não são suficientes para regulamentar as diversas infrações cometidas. Além da visível necessidade de criar mecanismos específicos e suficientes para exercer atividade punitivas dos indivíduos

delituosos. Tem se também, a percepção de que, a norma jurídica brasileira não tem acompanhado a evolução dos crimes cibernéticos visando coibir os crimes virtuais, o mundo virtual ainda é muito amplo e carente de leis específicas para punir tal delito, ou seja, se caracteriza um vazio normativo, que permita ao estado punir os infratores.

3 CRIMES CIBERNÉTICOS ATÍPICOS

A internet como ferramenta, trouxe diversos benefícios à sociedade, mas também criou diversas novas devastações, sendo uma delas a utilização da internet para a prática de novos delitos que importunam a paz social e os bons costumes, que também facilitou a prática de delitos antigos. Dentro desse tema, é imperioso consignar que ainda não se definiu um conceito uniforme de Delito Informático. Aliás, nem mesmo umas renomadas denominações estabeleceu, pois há quem o trate pela denominação de Criminalidade Mediante Computadores, Criminalidade do Computador, Delito Informático, Criminalidade da Informática, Delitos Cibernéticos, entre outros. A denominação ‘delitos informáticos’, pois dessa singela maneira não somente aquelas condutas praticadas no âmbito da internet ou em outras palavras o meio virtual, mas toda e qualquer conduta em que haja relação com sistemas informáticos, quer ser de meio, quer de fim, de modo que essa denominação abrangeria, delitos em que o computador seria uma mera ferramenta, sem a imprescindível conexão à Rede Mundial de Computadores. Aliás, no âmbito da internet, a denominação seria ‘delito cibernético ou telemático’. ‘Delitos informáticos’, então, seriam gênero, do qual ‘delito cibernético’ seria espécie. E em razão da recenticidade do assunto, outras denominações podem surgir com o amadurecimento da questão.

Interessa destacar que Tiedemann, já em 1985, chegou a definir:

> “Criminalidad Mediante Computadoras: se alude a todos los actos, antijuridicos según la ley penal vigente (o socialmente perjudiciales y por eso penalizables en el futuro), realizados com el empleo de un equipo automático de procesamiento de datos”. (Tiedemann, 1985 pág.487).

Porém o melhor conceito para ‘delito informático’ é o alcunhado pela Organização para a Cooperação Econômica e Desenvolvimento da ONU: “O crime de informática é qualquer conduta ilegal não ética, ou não autorizada, que envolva processamento automático de dados e/ou transmissão de dados”.

Entre as mais diferentes modalidades de delitos, os mais relevantes se consistem em sendo uma delas os Delitos Informáticos Puros, aqueles em que o indivíduo visa atingir ou danificar especificamente ao sistema de informática em todas as suas formas, sendo que a informática é composta principalmente do software, do

hardware (computador e periféricos), dos dados e sistemas e dos meios de armazenamento. Sobre a conduta (ou ausência dela) é visado exclusivamente ao sistema informático do sujeito passivo. São exemplos, atos de vandalismo virtual contra a integridade física do sistema em razão de acesso não autorizado – as condutas dos hackers e crackers – ainda não tipificadas no Brasil, além de algumas já previstas, como as hipóteses preconizadas na Lei n 9.609/98 (Lei de Proteção de Software). Rossini (2002, p. 139).

Se caracteriza também os Delitos Informáticos Mistos, em que o computador é mera ferramenta para a ofensa a outros bens jurídicos que não exclusivamente os do sistema informático. Alguns de seus exemplos são o estelionato, a ameaça e os crimes contra a honra, podendo imaginar-se, inclusive, homicídio por meio da internet (mudança à distância de rotas de aviões, alterações à distância de medicamentos com o desautorizado uso do sistema informático de um hospital).

Antes, porém, é de bom alvitre se recordar que bem jurídico é “aquele valor ético-social que o direito seleciona, com o objetivo de assegurar a paz social, colocando sob sua proteção para que não seja exposto a perigo de ataque ou lesões efetivas”

Wezel, apud Assis Toledo (1994) cita que*:*

> “a soma dos bens jurídicos constitui a própria ordem social, e por isso, o significado de um bem jurídico não deve ser apreciado isoladamente, mas sim, em conexão com toda a ordem social”. (Toledo, 1994, pág. 75)

Importante concluir, que, o Direito Penal tem por escopo fundamental a proteção de bens jurídicos (e não poderia ser de outra forma em um Regime Democrático de Direito). Ora, se aqui se aponta a necessidade da intervenção do Direito Penal na Informática, sustentando-se, inclusive, que há Delitos Informáticos, o que exatamente se busca proteger?

Se admitirmos a classificação acima, a indicação impostas dos bens jurídicos nos “Delitos Mistos” torna-se a não ser tarefa difícil, pois são classicamente consagrados, como no estelionato praticado por meio da internet, o bem jurídico protegido é o patrimônio; nos crimes de calúnia, injúria e difamação cometidos por meio da Rede, o bem jurídico que se busca cautelar é a honra; e assim com outras modalidades de delitos. Nos “Delitos Puros” os bens jurídicos a se proteger também são de fácil vislumbre, como nos de conduta atípica do cracker (que invade, altera ou destrói o que há no computador da vítima, podendo também vazar dados bancários

ou pessoais) o bem jurídico ainda continua sendo o patrimônio, pois tal conduta não deixaria de caracterizar o ‘dano informático’; contudo, na modalidade tipificada de ‘pirataria de software’, o bem jurídico protegido é a propriedade intelectual. Que se denota há um bem jurídico absolutamente permanente que é a Segurança Informática, que existe independentemente de bens jurídicos individuais e coletivos que possam coexistir concomitantemente em uma conduta típica praticada no âmbito aqui já estabelecido (internet). No tríplice classificação proposta por BORTONE (2000), e aqui admitida como a melhor, trata-se de um bem jurídico-penal de natureza DIFUSA. Isto porque, além de atingir um número indeterminado de pessoas, gera conflituosidade entre o interesse dos usuários da internet (incontáveis), aí incluídos os usuários comuns, além dos hackers (pichadores cibernéticos), crakers (punks cibernéticos) e o das grandes corporações, quer de empresas fornecedoras de bens e serviços, quer de provedores de acesso.

Por outro lado, um contra ponto surge dentro dos atos contra os dados ou programas de computador, que é a denominada espionagem informática. (Sieber, 1998) Fato que acontece por meio de alteração dos programas do computador, mantendo o computador em erro para o emprego de sabotagens e meios ardilosos de obtenção de informações, tais como se destaca, o Trojan, ou mais conhecido comumente como “cavalo de tróia”, este se caracteriza como uma espécie de “malware”; que é um termo genérico em que Klein Tobias, (2011) cita: “Malware são apelido criado para qualquer tipo de software malicioso projetado para prejudicar ou explorar qualquer dispositivo Serviço ou rede programável.” O que define muito bem com a finalidade como anteriormente foi dito, é um dos muitos meios que os Crackers utilizam para esse tipo sabotagem e espionagem, nesse caso podem recair sobre o criminoso as penas do artigo 156 do Código Penal, pena de reclusão que varia de 1 à 4 anos mais multa.

Outra vertente dentro dos atos contra dados do computador se foca na destruição total do programa do computador. Esta prática se tornou, ao longo da popularização da internet, uma prática comum, os vírus de computador são capazes das maiores atrocidades possíveis dentro da máquina, prejudicando em todo ou em parte a estrutura do sistema. As diversas práticas ligadas aos vírus ou malwares, começam a surgir na década de 90 e não param mais, atualmente grandes empresas são vítimas de constantes contaminações nos sistemas devido a novos vírus serem

criados praticamente todos os dias. No direito nacional ainda surgem dificuldades para sua tipificação, contudo já se enquadram certas situações como dano, 163 do CP, além da sanção cível para se restituir patrimônio, previsto no 159 do Código Civil de 2002.

A informática é um meio em que comumente são cometidos crimes contra direitos imateriais, direitos que dizem respeito à propriedade intelectual, literária e artística, e a propriedade industrial, que, seguindo o Direito Empresarial, explanado na obra de Fábio Ulhoa Coelho (2002), seria o conjunto de normas que dá: “a quatro bens imateriais a proteção: a patente, a invenção, a de modelo de utilidade, o registro de desenho industrial e o de marca. O empresário titular desses bens tem o direito de explorar economicamente o objeto correspondente, com inteira exclusividade”. No Brasil o Instituto Nacional da Propriedade Industrial concede a mercê esses direitos industriais (INPI).

A propriedade intelectual é um bem jurídico protegida pela Lei de Direitos Autorais, hoje regulada pela lei 9609 de 1998. Consoante, a propriedade industrial já vem protegida com a própria Constituição Federal de 1988, no artigo quinto, XXIX, sendo reformulada pela lei 9279/96 que regula direitos e obrigações relativos à propriedade industrial, nessa lei os artigos 183 a 195 tipificam os crimes contra patente de invenção, sendo delitos que podem ser cometidos pela internet.

Nesse ponto tentamos enfatizar de uma forma mais sucinta que crimes na internet atingem os mais variados ramos e devem ser protegidos de forma efetiva, pensando-se em todas as hipóteses de delitos possíveis. Os bens imateriais também estão a mercê, destes atos, sendo alvos de práticas criminosas na internet, mas o que poucos sabem é que já existe uma tipificação para esses crimes, desse modo, segundo Romano (2019), configura-se como crime contra a propriedade imaterial "aqueles que ocorrem contra a atividade criadora das pessoas, que é fruto de seu intelecto e cuja proteção constitucional está prevista no artigo 216 da Constituição Federal". A utilização de uma nova legislação que reúna todos esses atos ilícitos de uma forma una e indivisível se tem mostrado muito necessária para uma melhor atuação do operador do Direito, sem uma completa reunião de todos os ilícitos penais em uma só carta não será possível um melhor controle dos ilícitos, sendo este um ramo novo do Direito Penal.

Todavia, apontaremos os elementos da Segurança Informática:

A) Integridade, e o princípio de integridade refere-se a manutenção das condições iniciais das informações de acordo com a forma que foram produzidas e armazenadas. Ou seja, a informação mantém sua origem e ela não pode ser alterada, assim somente pessoas autorizadas poderão acessar e modificar os dados do sistema. – a informação deve ser fidedigna e completa e somente o usuário pode mudá-la. (KLEIN, 2011)

B) Disponibilidade, esse princípio diz respeito à eficácia do sistema e do funcionamento da rede para que seja possível utilizar a informação quando necessário. Ela deve ser hospeda em um sistema à prova de falhas lógicas e redundantes. – O usuário deve ter a informação no momento em que necessite. (KLEIN, 2011)

C) Confidencialidade, como síntese, É o modo de garantir que a informação estará acessível apenas para pessoas autorizadas. A principal forma de mantê-la é por meio da autenticação, controlando e restringindo os acessos. Ela impõe limitações aos milhares de dados sigilosos que as empresas possuem. Sem a confidencialidade, as empresas ficam vulneráveis a ciberataques, roubo de informações confidenciais e até utilização de dados pessoais de clientes, o que pode causar diversos prejuízos, inclusive financeiros. – ninguém, sem consentimento, deve ter acesso ou divulgar a informação. (KLEIN, 2011)

D) Autenticidade, este processo realiza a tarefa de identificar e registrar o usuário que está enviando ou modificando a informação. Ou seja, autenticidade é quando um usuário vai manipular algum dado e ocorre uma documentação sobre essa ação.

Todos esses métodos são importantes para garantir a segurança das informações corporativas das possíveis ameaças, que podem ter origens tanto externas quanto internas. Elas podem ser uma pessoa, um evento ou uma ideia capaz de causar danos ao sistema. (KLEIN, 2011)

Constatando a ausência de qualquer um desses elementos, a própria função da internet será ineficaz e não alcançará todas as suas possibilidades. Não passará de mais um simples meio de comunicação, como o rádio ou a televisão. Inquestionavelmente, o poder de alcance e de informações da internet é muito maior, pois, transformou sobremaneira a interatividade da sociedade moderna e não pode, e nem deve ficar adstrita a somente uma de suas funções visando sempre a evolução

sobremaneira a deixar tudo mais prático – a comunicação. A Rede Mundial de Computadores não tem limites, desde que não seja tolhida em sua essência. (Lawrence Roberts e Thomas Merril, 1995)

Importante citar também, por motivos de conhecimento, que delitos cometidos no âmbito digital, muitas vezes são nomeados como: crimes cibernéticos, crimes digitais, crimes eletrônicos, crimes da informática, crimes cometidos na internet, cibercrimes, fraudes eletrônicas, delitos computacionais, dentre outros, mas todos eles referem-se, à prática delituosa cometida no meio digital. Assim surge-se a necessidade de classificar os diversos tipos de crimes cometidos no meio ambiente digital. Existem diversas classificações doutrinárias a respeito de tal tema que é amplamente discutido e apontado por diversos autores.

Para Higor Vinicius Nogueira Jorge (2012) e Emerson Wendt (2012), existem as ações prejudicais atípicas e os crimes cibernéticos. As ações prejudiciais atípicas, são aquelas condutas que causam prejuízo ou transtorno para vítima através da rede mundial de computadores, mas não são tipificados em lei. Por sua vez os crimes cibernéticos se dividem em “crimes cibernéticos abertos” e “crimes exclusivamente cibernéticos”.

Como é o caso da Lei Carolina Dieckman:

> A Lei Carolina Dieckmann é a Lei Nº 12.737/2012 e é uma alteração no Código Penal Brasileiro voltada para crimes virtuais e delitos informáticos. Com o avanço da tecnologia e a democratização e o acesso facilitado às redes sociais, o sistema judiciário brasileiro viu a necessidade de tipificar crimes cometidos no ambiente virtual. são aqueles que necessariamente precisam do meio da informática para cometer tal crime (como é o caso do crime de invasão de dispositivo informático, artigos 154-A e154-B do código penal, introduzido pela Lei 12.735/2012, conhecido como Lei Carolina Dieckmann).

Outra parte da doutrina entende que os crimes cibernéticos podem ser estudados, levando-se em consideração o papel desempenhado pelo computador no contexto da prática do ato ilícito. Nesse sentido, conforme esclarece Pinheiro (2013, apud FERREIRA, 2001).

As questões apresentadas representam um verdadeiro desafio ao Ministério Público, que além de ser o titular exclusivo da ação penal pública (art.129, I, da Constituição Federal), também tem por função a defesa do regime democrático (art.128, caput, da Constituição Federal). E não se pode negligenciar que a livre iniciativa é um dos fundamentos da República Federativa do Brasil (art.1º, inciso IV,

última parte, da Constituição Federal). Se de um lado a modernidade traz benefícios inquestionáveis à sociedade, também traz, de outra banda, enormes desafios àqueles que têm por função assegurar a paz social, dentre eles, com relevo, o Ministério Público, e os órgãos executivos de combate ao crime como a segurança pública.

4 APLICABILIDADE DE PRINCÍPIOS AOS CIBERCRIMES

Levando em consideração a ausência de lei específica para tal caso, bem como, a insuficiência das disposições da Lei n. 9.296/96, o aumento da incidência de infiltrações clandestinas em computadores pessoais nos mostra a cada dia a dificuldade, no que diz respeito a garantia constitucional do direito à privacidade. Vale ressaltar ainda o elevado grau de intromissão na intimidade e na vida privada, com o consequente incremento dos riscos de abuso, denomina-se de suma importância a sua disciplina em lei, com clara indicação dos requisitos, procedimentos e cautelas a serem observados em seu deferimento. (ROSA, 2018).

Ressalta observar que torna-se bastante complexo o acompanhamento das várias ferramentas disponibilizadas via internet para os usuários, conforme o autor cita anteriormente, no sentido de afirmar a inviabilidade da infiltração clandestina em computadores sendo mais frequentes de uso pessoal, porém, tem se percebido uma ferramenta mais atual utilizada, que é a demanda do estudo em tela, pois, com o avanço desenfreado do mundo cibernético, não se utiliza mais a invasão clandestina da máquina do suspeito, podendo, tão somente coletar informações em suas redes sociais como página do Facebook ou Instagram exemplo.

Com estes dados em mãos haveria maiores possibilidades de se chegar aos verdadeiros culpados de algum delito, promovendo maior índice de pacificação social através da aplicabilidade da justiça, e levando aquele agressor a sua devida punição prevista em legislação específica, como impacto resultante, haveria a possibilidade de estar diminuindo a sensação de impunidade que verbaliza nossa população sempre em que não se consegue chegar à comprovação de autoria delitiva dos crimes. Contudo, carecemos de normas regulamentadoras das ações policiais na obtenção de dados de forma ágil e versátil, viabilizando a melhor aplicabilidade do poder executivo, viabilizando instruções e estratégicas melhores para agentes aplicadores da lei. (OLIVEIRA, 2012).

Quando se tem ciência dos vários projetos de lei que tentaram regulamentar a presente situação em nosso ordenamento jurídico, muitos profissionais do Direito

tentaram enquadrar essas práticas ilícitas e atípicas que comumente vem ocorrendo e, por falta de uma legislação especifica, acabam não sendo punidas.

Visando essa efetivação do jus puniende do Estado é que surgem algumas ideias acerca de como se deve proceder diante desses fatos inovadores, apesar de muitos projetos, nenhum foi efetivamente difundido, chegando a ter seu uso efetivado. os mais variados projetos de lei são inventados, contudo, só teremos uma completa efetivação da prevenção aos crimes e punição dos mesmos se o projeto for transformado realmente em lei, só assim teremos um meio de combater essas práticas que se escondem na defasagem do ordenamento jurídico interno. Vejamos então alguns dos projetos de leis que ora foram criados em nosso país:

PL 1.070/1999 – Dispões sobre crimes oriundos da divulgação de material pornográfico através de computadores.

PL 3.258/1998 – Dispõe sobre perpetrados por meio de redes de informação, caracterizando como crime a divulgação pela internet e demais redes de computadores de material pornográfico, instruções para fabricação de bombas caseiras e textos que incitam e facilitam o acesso a drogas ilegais.

PL 3.493/1997 – Acrescenta artigos ao código penal, incluindo, no capitulo dos crimes contra a privacidade, a violação da intimidade, mediante processo tecnológico, e o abuso da informática, com a divulgação de dados pessoais alheios, fichário automatizado ou banco de dados.

PL 4.412/1998 – Acrescenta artigos à lei 8.069 para dispor sobre crimes de abuso sexual, incluindo a pena de reclusão para quem pratica conjunção carnal, atentado violento ao pudor, ato libidinoso, incluindo na mesma pena quem persuade, induz ou atrai adolescente a praticar crime.

PL 84/1999 – Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providencias. Caracteriza como crime os ataques praticados por Hackers e Crackers, em especial as alterações de home pages e a utilização de senhas.

PL 3.891/2000 – Dispõe sobre o registro de usuários pelos provedores de serviços de acesso a redes de computadores, inclusive a internet, obrigando os provedores de serviços da internet a manterem registros de seus usuários e dados referentes a cada transação atendida pelo provedor, para solucionar o problema da

identificação do usuário em caso de utilização ilícita da rede, cometida, em geral, por hackers ou crackers.

PL 76/2000 – apresentado por Renan Calheiros, define e tipifica os delitos informáticos e da outras providencias.

PL 137/00 – Apresentado pelo senador Leomar Quintanilha, estabelece nova pena aos crimes cometidos com a utilização de meios de tecnologia de informação e telecomunicações.

PL 5460/01 – Altera os artigos 240 e 241 da lei 8069, incluindo como crime de produção de atividade fotográfica ou de qualquer outro meio visual utilizando-se de adolescente em cena de sexo explícito ou simulado, agravando pena sendo a vítima criança.

PL 6384/02 – Acrescenta artigo 232-A e parágrafo único ao artigo 239, modifica os artigos 236, 241, 242 e 243 da lei 8069. Agrava pena para crimes praticados contra a criança e o adolescente, por ação ou omissão, incluindo a exploração do menor para obtenção de vantagem patrimonial e a pratica de pedofilia.

PL 480/03 – Dispõe sobre o cadastramento dos usuários de serviços de internet e disponibilização de dados a autoridade policial e da outras providencias.

PL 121/2008 – Apresentado pelo senador Magno Malta, proíbe as empresas de cartões de pagamento de autorizarem transações relacionadas com jogos de azar e pornografia infantil via internet.

Os mais variados projetos de lei são inventados, contudo, só teremos uma completa efetivação da prevenção aos crimes e punição dos mesmos se o projeto for transformado realmente em lei, só assim teremos um meio de combater essas práticas que se escondem na defasagem do ordenamento jurídico interno. Tendo em vista essas dificuldades o que muitos tribunais fazem é utilizar as normas já existentes para enquadrar crimes na internet nessas condutas usando de analogias que também é um dos princípios do Direito, contudo, muitas vezes isso não é viável, ou não existe uma pena justa, um mal na internet algumas vezes pode atingir proporções muito maiores que no mundo real, a discriminação e injúria nessa rede mundial de computadores pode atingir proporções mundiais, criando traumas dificilmente esquecidos pelos agentes passivos do ato criminoso.

Alguns projetos de lei já estão em trâmite, mas ainda não saíram do papel, sendo necessária uma celeridade nessa questão, a sociedade está mudando, o

Direito, como também é ser mutável, deve se adequar as novas demandas sociais, sendo inexistente a falta de punição daqueles que se acobertam pela defasagem e lacunas de nosso Código Penal Brasileiro. Visando ser questões de suma importância que necessitam de um cuidado e de serem resolvidas o quanto antes.

Adentrando de modo global, os crimes na internet são debatidos pelos poderes soberanos ao redor do mundo nos quais muitos deles já buscam uma maneira de coibir essas práticas, ideia interessante é a da Convenção de Budapeste que integra vários países, submetendo-os as leis ali tratadas, dando poderes de atuação em seus países signatários, segundo Capez: “a ideia é válida, mas é necessário um certo cuidado, toda a convenção e suas leis devem ser estudadas de maneira a não colidirem com os princípios fundamentais previstos em nossa Constituição Federal, caso colidam, não deve ser subscrita por nosso país”. (Capez, 2004)

Segundo sites de grande relevância mundial, a Convenção de Budapeste foi criada em 2001, na Hungria, pelo Conselho da Europa, englobando mais de 40 países e tipifica os principais crimes cometidos na internet. A convenção objetiva proteger a sociedade contra a criminalidade no ciberespaço, através de legislação adequada e das demais melhoria de cooperação internacional, reconhecendo a necessidade de cooperação entre os Estados e as indústrias privadas para a prática reiterada no combate contra estes atos delituoso. A convenção traz consigo os crimes na internet tipificando-os como infrações contra sistemas e dados informáticos, infrações relacionadas com computadores (hardware), infrações relacionadas com o conteúdo, pornografia infantil e infrações relacionadas com a violação de direitos autorais. Apesar do objetivo ser de reprimir e reduzir os crimes na internet, o projeto visa ter tendência a não oferece uma base muito segura, conforme cita o Ministério das Relações Exteriores, em sua nota conjunta ao Ministério da Justiça e da segurança Pública; “um poder soberano não pode intervir em outro, tais medidas gerariam desconforto dentro das relações internacionais, acredito que proceder dessa maneira não é viável, melhor seria uma padronização da Convenção de Budapeste, aliada a uma atuação de uma policia internacional voltada para crimes na internet internacionais.”

Seguindo mais adiante para os Estados Unidos, podemos dizer que diferente de nós, ele tem se baseado no commom Law, sendo este, o direito que se desenvolve

através de decisões de tribunais, em outras palavras a Jurisprudência Norte-Americana, e não por atos legislativos como aqui no Brasil.

A recente tentativa de eliminar a pornografia na internet foi proposta seguida a lei de Decência de Comunicações de 1996, buscando tornar a internet um ambiente mais saudável para o acesso de jovens, contudo, os legisladores não tinham um conhecimento sobre a Internet, logo, a lei se tornou ineficaz. Esta Lei foi criada com o objetivo de disciplinar o exercício do direito de resposta ou retificação do ofendido em matéria divulgada, publicada ou transmitida por veículo de comunicação social como a internet.

Com a internet trazendo muitas dificuldades devido a sua despersonalização, pois não é se caracteriza como algo material, vive em sua própria rede, por isso é tão difícil regulamentar e punir agentes criminosos que atuam utilizando esta tecnologia, porém nem sempre de mal a internet é composta, a mesma tem como importância fundamental em gerar o aumento de comunicação entre as economias mundiais, gerando maiores possibilidades e conhecimentos para o homem, além de fornecer informações a nível praticamente instantâneas sobre quaisquer eventos que estejam acontecendo ao redor do mundo. Não obstante dizer que Internet pode ser comparado a um ser vivo, pode ser um “Estado” de todos que está se formando, logo, precisa de regulamentação e de regramento, tanto nacional quanto a âmbito internacional, os países devem pensar e agir em matéria disso o mais rápido possível, antes que as coisas não percam o controle e que a internet realmente acabe se tornando uma “terra de ninguém”. Pois Diante do parâmetro nacional, a falta de normatização acaba gerando insegurança jurídicas para a população e não unicidade nas decisões dos tribunais no que diz respeito a esses crimes, afinal, no Direito Penal existe o princípio do in dúbio pró réu (em dúvida beneficia-se o réu), unido aos princípios de anterioridade e da legalidade, o que pode tornar ainda mais dificultoso proibir práticas e atos que não são definidas especificamente por uma legislação norteadora desses fatos sociais comuns no cotidiano dos brasileiros e do Mundo.

5 CONSIDERAÇÕES FINAIS

O presente estudo trouxe à luz o tema sobre as evoluções de crimes virtuais e seus impactos na sociedade. Justificando-se pela grande dificuldade de punir os infratores de crimes cibernéticos uma vez que tomando para si o êxito do fato delituoso, posteriormente podendo ser, um agente causador em potencial que enfatiza o aumento crescente de crimes desta modalidade em nosso país, aponta-se também a falta de legislação específica para saneamento e contenção dessas atividades criminosa, fazendo-se assim crescer um grave problema jurídico e social.

Nessa perspectiva, a presente pesquisa buscou respostas para o seguinte problema: Quais são as principais dificuldades encontradas pelos operadores do direito no que diz respeito a punir os infratores? Tendo como objetivo geral entender as principais dificuldades encontradas pelos operadores do Direito no momento de determinar autoria e assim punir os infratores. Para tanto, três capítulos descreveram, à luz da teoria, sobre A Relação do Direito e a Informática, os principais crimes cibernéticos que são atípicos em decorrência de ausência de lei específica e as diversas aplicabilidade dos princípios de legalidade, reserva legal e analogias aos crimes cibernéticos.

Sobre a Relação entre o Direito e a informática Surgiu como um marco inicial em plena guerra fria, sendo utilizada como uma espécie de arma norte-americana de informação militar, tendo em si a principal função de interligar todas centrais de computadores dos postos de comandos táticos americanos. Sendo uma suposta prevenção de alguma atividade surpresa ofensiva russa. Com o passar do tempo a internet vem proporcionando que milhões de computadores e também dispositivos móveis e não móveis das mais diversas categorias, contribuindo assim para o acesso a todo tipo de informação e transferência de dados, tanto comunicativos, quanto informativos, business e comercial.

E neste sentido surge o Direito como uma ferramenta de controle de segurança, buscando estudar as implicações e os problemas jurídicos surgidos com a utilização das modernas tecnologias da informação. E com o passar do Tempo esta disciplina vem ganhando seu espaço e se consolidando como um novo ramo das ciências jurídicas que sobretudo tem o objetivo de sanar e regularizar a necessidade de adaptação de normas em vigor visando regular as relações neste ambiente virtual.

Em relação aos mais variados crimes cibernéticos atípicos, ou seja, uma conduta que não é expressa por lei. Dentre elas destaca-se Delitos Informáticos Puros, que são aqueles em que o indivíduo visa atingir ou danificar especificamente ao sistema de informática em todas as suas formas, principalmente do software (Programas), ou hardware (computador e periféricos), dos dados e sistemas e dos meios de armazenamento da máquina. E também se destaca os Delitos Informáticos Mistos, em que o computador é mera ferramenta para a ofensa, estelionato, ameaça e os crimes contra a honra, e entre outros.

A respeito dos elementos de Segurança da Informática, que são métodos importantes para garantir a segurança das informações corporativas e individuais das possíveis ameaças, que podem ter origens tanto externas quanto internas. Sendo elas o princípio da Integridade, Disponibilidade, Confidencialidade e Autenticidade. Constatando a ausência de qualquer um desses elementos, a própria função da internet será ineficaz e não alcançará todas as suas possibilidades e tornando-se um meio inseguro de comunicação e transferência de dados.

Mediante ao estudo realizado, a aplicabilidade de princípios, analogias visando o combate de crimes virtuais, quando se tem a ciência da necessidade de elaboração de projetos de lei que tentam regulamentar as condutas delitivas virtuais e por muitas vezes os profissionais do Direito acabam não levando a punições legais esses criminosos, por falta legislação especifica. À luz das teorias, exploradas na fundamentação teórica desta pesquisa bibliográfica, tornando-se possível afirmar que os objetivos específicos e geral foram alcançados neste estudo científico demonstrando e discorrendo brevemente sobre os objetivos propostos.

Por mais que tenham ficado explícitos os a legislação Brasileira tem escassez de leis e normatizações que regulam sobre crimes em âmbito virtual específico, por meio deste estudo bibliográfico, é possível avançar em novos estudos que possibilitem futuras bases de pesquisas sobre o tema proposto. Assim, como propostas para futuras pesquisas, sugere-se que novos estudos mais aprofundados possam ser realizados como: O combate de crimes virtuais relacionados a pornografia Infantil em seu Território Internacional; Evoluções de Sistemas Internacionais contra o combate ao Terrorismo Virtual.

REFERÊNCIAS

BARATTA, Alessandro. **Criminologia Crítica e Crítica do Direito Penal. Introdução à Sociologia do Direito Penal.** Alemanha: Editora Renavan, 2002.

BRASIL. **constituição da república federativa do brasil de 1988**. disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.html. acesso em 10 outubro. 2018.

Barriuso Ruiz, Carlos. **Interacción del Derecho y la informática**. 1ª ed., Dykinson, Madrid, 1996.

BORTONE, João. **Segurança na Era da Intemet. PC Master**. São Paulo, Ano 3, n. 10, março 2000. 114p.

CARDOSO, Manoel Santana. **A Lei de informática como política pública de fomento às tecnologias da informação e comunicação (TICS) no país: uma análise da interação entre a indústria e a academia.** Brasília: Mestrado em Direitos Humanos, Cidadania e Violência, 2016.

CAPEZ, Fernando. **Direito penal: parte geral.** São Paulo: Saraiva, 2004.

COELHO, Betty. **Contar histórias: uma arte sem idade**. São Paulo: Ática, 2001.

COELHO, Fábio Ulhoa. **Manual de Direito Comercial – Direito de Empresa.** 21 Edição. Editora Saraiva, São Paulo. 2009.

DELGADO, Mauricio Godinho. **Curso de direito do trabalho**. São Paulo: Rede Virtual de Bibliotecas, 2007.

FERREIRA, Ivete Senise. **A criminalidade informática.** LUCCA, Newton.; SIMÃO FILHO, Adalberto (Coord.). Direito e internet. Bauru: Edipro, 2001.

KLEIN, Tobias. **A Bug Hunter's Diary – A Guided Tour Through The Wilds of Software Security.** Londres: No Starch Press, 2011.

LESSIG, Lawrence. **Code and other Laws of Cyberspace.** New York: Basic Books, 1999.

LESMES SERRANO, Carlos. **"Las nuevas tecnologías y la Administración de Justicia. La Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil"**. Obra coletiva Derecho de Internet: Contratación Electrónica y Firma Digital, Aranzadi. Navarra, 1997.

LESMES SERRANO, Carlos. **Derecho penal administrativo: ordenación del territorio, patrimonio histórico y médio ambiente.** Espanha. Editorial Comares, 1997.

MPF, Ministério Público Federal. 2ª câmara de coordenação e revisão, ata da sessão de revisão. **Matéria Criminal e Controle Externo da Atividade Policial.** Brasília (DF), 26 de maio. 2014. Disponível em: https://www.mpf.mp.br/atuacao-tematica/ccr2/revisao/atas-de-revisao-1/atas/Ata_599_26_05_14.pdf. Acesso em 20 outubro. 2022.

OLIVEIRA, Edmundo. **Novos rumos da vitimologia: o crime precipitado pela vítima.** Boletim IBCCRIM. São Paulo, v.9, n.107, outubro. 2012. 17p.

PAESANI, Liliana Minardi. **Direito de Informática.** São Paulo: Atlas. 2006

PEREIRA, Marcelo Cardoso. **Breves considerações sobre Direito Informático e Informática Jurídica.** Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 6, n. 51, 1 out. 2001. Disponível em: https://jus.com.br/artigos/2255. Acesso em: 10 outubro. 2022.

ROSSINI, Augusto Eduardo de Souza. **Brevíssimas considerações sobre delitos informáticos.** Caderno Jurídico da Escola Superior do Ministério Público do Estado de São Paulo, 2002. 139p.

ROMANO, Rogério Tadeu. **Processo e julgamento dos crimes contra a propriedade imaterial.** Disponível em: https:/ /www.jfrn.jus.br/institucional/bibliotecaold/doutrina/Doutrina257_Processo_e_JulgamentoCrimes.pdf. Acesso em: 25 set. 2019.

ROSA, Fabrízio. **Crimes de Informática.** Campinas: Bookseller, 2008.

TIEDEMANN, Klaus. **Criminalidad mediante computadoras.** Alemanha: E.P.U, 1985. 487p.

TOLEDO, Francisco de Assis. **Princípios básicos do direito penal.** 5 ed. 7. tiragem. São Paulo: Saraiva, 2000.

WEZEL, Hans. **Derecho penal alemán: parte general. Traducción de Juan Bustos Ramírez y Sergio Yáñez Pérez.** Santiago: Jurídica de Chile, 1997.

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