FACULDADE VIASAPIENS – FVS
CURSO DE GRADUAÇÃO EM DIREITO

FRANCISCO ENAGIO ARAUJO SILVA

CRIMES DIGITAIS E SEUS IMPACTOS NA SOCIEDADE CONTEMPORÂNEA

Tianguá – CE
2023

FRANCISCO ENAGIO ARAUJO SILVA

CRIMES DIGITAIS E SEUS IMPACTOS NA SOCIEDADE CONTEMPORÂNEA

Monografia apresentada a Faculdade ViaSapiens – FVS como requisito parcial para a obtenção do título de Bacharel em Direito.

Orientador(a): Professor (a) Francisco Danilo de Souza Gomes.

Orientador metodológico: Professor Esp. Francisco Danilo de Souza Gomes.

Tianguá – CE

2023

FACULDADE ViaSapiens
A IDENTIDADE DO CONHECIMENTO

FACULDADE VIASAPIENS – FVS
ATA DE DEFESA DE MONOGRAFIA DO CURSO DE DIREITO

Em 25 de novembro de 2023, às 08:00 h, no Auditório 02 da Faculdade ViaSapiens, de modo presencial, compareceram para a **DEFESA PÚBLICA DE MONOGRAFIA** do curso de graduação Direito, requisito obrigatório para a obtenção da aprovação na disciplina de Trabalho de Conclusão de Curso II, o(a) aluno(a): **FRANCISCO ENAGIO ARAUJO SILVA,** tendo como título do Trabalho **CRIMES DIGITAIS E SEUS IMPACTOS NA SOCIEDADE CONTEMPORÂNIA**, e os professores que constituíram a Banca Examinadora:

a) Professor(a)-orientador(a): Prof. Esp. Francisco Danilo de Souza Gomes;
b) Professor(a)-examinador(a): Prof. Esp. Francisco Maxvânio Parente Vasconcelos;
c) Professor(a)-examinador(a): Prof. Esp. Rodrigo Ramos Freire de Castro.

Após a apresentação da Monografia e as observações dos membros da banca avaliadora, ficou definido que o trabalho foi APROVADO, com média 10, (DEZ), a partir das seguintes notas:

EXAMINADOR(A)	NOTA	VISTO
Prof. Esp. Francisco Danilo de Souza Gomes;	10	
Prof. Esp. Francisco Maxvânio Parente Vasconcelos;	10	
Prof. Esp. Rodrigo Ramos Freire de Castro.	10	

Eu, **Francisco Danilo de Souza Gomes**, professor(a)-orientador(a), lavrei a presente ata, que segue assinada por mim e pelos demais membros da Banca Examinadora.

Reformulações:
(X) Não.
( ) Sugeridas
( ) Exigidas

Professor(a) Esp. Francisco Danilo de Souza Gomes
Orientador(a)

Professor(a) Esp. Francisco Maxvânio Parente Vasconcelos
Examinador(a)

Professor(a) Esp. Rodrigo Ramos Freire de Castro
Examinador(a)

Francisco Enagio Araujo Silva – ALUNO (A)

Dados Internacionais de Catalogação na Publicação
Ficha catalográfica elaborada pela Biblioteca da Faculdade ViaSapiens
com os dados fornecidos pelo(a) autor(a)

A658c

ARAUJO SILVA, Francisco Enagio .

Crimes Digitais e Seus Impactos na Sociedade Contemporânea : / Francisco Enagio ARAUJO SILVA - 2023.

43 f.

Trabalho de Conclusão de Curso (graduação) - Faculdade ViaSapiens, Bacharelado em Direito. Tianguá. 2023

Orientação: Prof(a) Esp. Francisco Danilo de Souza Gomes

1. Crimes. 2. Digitais. 3. Ordenamento Juridico. 4. Poder Judiciário

. I. Titulo.

Dedico esse estudo monográfico a Deus, minha esposa Michele e minha mãe Maria do Carmo.

AGRADECIMENTOS

Jesus, porém, respondeu-lhes: Em verdade vos digo que, se tiverdes fé e não duvidardes, não só fareis o que foi feito à figueira, mas até, se a este monte disserdes: Ergue-te e lança-te ao mar, isso será feito;
Mateus 21:21

Através desse versículo aponto como é extremamente importante buscarmos a fé para construir tudo de bom que buscamos para nós, A minha trajetória até aqui, foi construída sobre muitos desafios e obstáculos, mas nenhum deles me fez desistir. Deus esteve comigo e sempre estará em toda a minha trajetória de estudos e em geral, na minha vida, tenho certeza de que a conclusão desse curso é apenas uma, diante das inumes conquistas que irei realizar.

O desenvolvimento desse trabalho de conclusão de curso obteve ajuda de várias pessoas, dentre as quais agradeço:

Minha Esposa, que sempre esteve comigo nesta jornada e principalmente naqueles momentos mais difíceis os quais me sentia desmotivado.

Minha Mãe, que sempre me incentivou a buscar os estudos como fonte de conquista.

A Faculdade Via Sapiens, e a todo o quadro de professores os quais fizeram parte da construção do meu aprendizado, e digo que todos foram muito importantes nesta etapa decisiva da minha vida.

“Só os bons sentimentos podem unir-nos uns aos outros; nunca o interesse mesquinho determinou laços firmes”.

Auguste Comte

RESUMO

Este Trabalho aponta o surgimento dos crimes digitais e o conceito evolutivo até os dias atuais e suas modificações com todos os processos de desenvolvimento tecnológico. Dessa forma, explica o quanto os crimes cibernéticos vêm se modificando constantemente e em grande proporção, principalmente no Brasil, país que nos últimos anos vem concentrando de acordo com pesquisas e estudos, grande escala de criminosos e ataques digitais através das grandes organizações criminosas desse setor. Ademais busca observar o comportamento do ordenamento jurídico brasileiro diante do atual senário desses tipos de crimes. Nesse sentido analisa como o poder judiciário conduz o patrocínio das investigações, sobre a temática e a atuação dos agentes de segurança para o combate dos crimes cibernéticos diminuindo desse modo os impactos negativos na sociedade.

Palavras-chave: Crimes; Digitais; Ordenamento Jurídico; Poder Judiciário.

ABSTRACT

This work points out the emergence of digital crimes and the evolutionary concept up to the present day and its modifications with all the processes of technological development. In this way, it explains how much cybercrimes have been changing constantly and in large proportions, especially in Brazil, a country that in recent years has been concentrating, according to research and studies, a large scale of criminals and digital attacks through large criminal organizations in this sector. In addition, it seeks to observe the behavior of the Brazilian legal system in the face of the current senarium of these types of crimes. In this sense, it analyzes how the judiciary conducts the sponsorship of investigations, on the subject and the performance of security agents to combat cybercrimes, thus reducing the negative impacts on society.

Keywords: Crimes; Digital; Legal Order; Judiciary.

LISTA DE SIGLAS

CF88 – Constituição Federal de 1988.

STF – Supremo Tribunal Federal.

STJ – Superior Tribunal de Justiça.

PF – Polícia Federal

CNB – Colégio Nacional Brasileiro

EUA – Estados Unidos América

SUMÁRIO

1. INTRODUÇÃO

O espaço virtual é um mundo que proporciona muita riqueza, e de fato onde existe riqueza há crime. O objetivo desse trabalho é expor ao leitor o grande perigo proporcionado pelos inúmeros crimes os quais sugiram e vem surgindo, devido ao enorme acesso pela população, à internet, bem como destacar o quanto a leis evoluíram e, deverão continuar evoluindo com o advento da evolução tecnológica.

Sem sombra de dúvidas o processo de globalização trouxe inúmeras e profundas modificações para a sociedade contemporânea. O mundo virtual através do surgimento da internet é algo que foi criado, mas que não é entendido pelos seus usuários, é algo que se diga de passagem, não existe um governo limitador, é o maior processo de anarquia criado pelas mãos e intelecto do homem.

Essa ideia de ser global gera na sociedade da informação o rompimento de barreiras econômicas, científicas e tecnológicas entre os países, por sua vez integrando sociedades. Esse processo de globalização iniciado ainda na metade do século XX, gera também uma sociedade do conhecimento, vive-se por tanto uma economia global e informacional.

A composição desse trabalho irá se empenhar em discutir os impactos dos crimes digitais no ordenamento jurídico brasileiro e como este deverá ser adaptado ao mundo tecnológico e as realidades sociais. A promulgação da lei 12.737 de 2012 é o primeiro passo para o combate a esses tipos de crimes. Merece discussão aqui também, além das tipificações dos crimes digitais, outras questões diretamente afetadas pelas práticas desses crimes tecnológicos, a grande rapidez com que esses crimes se propagam, os reais interesses buscados pelos criminosos, a dificuldade de identificação e investigação criminosa, a demanda de profissionais capacitados para evidenciar as autorias ilícitas que são bastante difíceis de identificar.

É relevante o interesse jurídico, social e educacional no mundo contemporâneo de expor o quanto o senário virtual é perigoso se utilizado de forma desordenada e sem o conhecimento adequado por quem está utilizando a internet, pois mesmo que a legislação busque abarcar os diversos tipos de crimes cometidos nesse ambiente, ainda sim a impunidade prevalece, não pelo fato de os agentes da lei agirem com arbitrariedade, mas pelo simples fato de que são diversos os motivos os quais ficam difíceis a identificação de determinados atos ilícitos nesse ambiente.

A todo momento surge inúmeros criminosos no mundo virtual e consequentemente dezenas de milhares de vítimas, leis são violadas e direitos são suprimidos. Dessa forma, o ambiente digital ao passo que é muito útil ao mundo moderno também traz consigo enormes perigos a quem precisa estar conectado e necessita realizar suas atividades diárias, seja com relação ao trabalho, a busca por lazer ou até mesmo para melhorar a qualidade de vida etc.

Assim, entende-se que a sociedade é um organismo em constante mudanças e na era da tecnologia é notório as mutações surgindo, a conexão virtual dita comportamentos e traça perfis humanos e cada vez mais cria costumes. Falar sobre os crimes informáticos no mundo contemporâneo é muito útil para todos. Hoje a internet confirma ser o principal meio de comunicação entre os povos, a necessidade de se estar conectado no dia a dia faz com que as transferências de informações transformem a vida cotidiana dos indivíduos conectados.

Ao passo que a sociedade se desenvolve e sofre mutações o ordenamento jurídico deverá ser ajustado para fatos inéditos, é o que está acontecendo atualmente, a revolução tecnológica força a todo momento as mudanças do direito, certamente o que começou com a revolução industrial tomou proporções assustadoras e hoje certamente não é difícil acreditar que daqui a mais alguns anos o que hoje vemos como crimes virtuais que possuem pouca semelhança com os crimes do mundo real irão se confundir, e isso possivelmente deva até facilitar as investigações para desvendar os crimes informáticos.

Diante de tudo que foi exposto compreende-se a necessidade de traçar uma linha de evolução histórica sobre a internet e os crimes nesse espaço, bem como explicar como o que começou com o intuito de ser um eficiente meio de comunicação, e é, tornou-se o ambiente ideal para a atuação dos criminosos cibernéticos, diante disso traça-se o objetivo geral de abordar os impactos causados por esse tipo de crimes, no mundo econômico, político e social e no ordenamento jurídico brasileiro. Nesse sentido, para alcançar a discussão da problemática e atingir o objetivo específico do trabalho, foram estabelecidos os seguintes parâmetros: explicar a evolução histórica de crimes digitais, conceito desses crimes, dados sobre crimes digitais no Brasil, marco civil da internet, condutas informáticas que são caracterizadas como crime, fraude informática e uso abusivo de dispositivos, relação entre direito penal e crime digital, artefatos e técnicas para prática dos crimes cibernéticos e investigação dos crimes cibernéticos.

A natureza metodológica desse trabalho é edificada com base em uma abordagem qualitativa uma vez que ele será construído com base em pesquisas bibliográficas, dispositivos normativos, dissertações, revistas eletrônicas e artigos científicos, criando desse modo um elo entre os apontamentos para a descrição e construção de explanações objetivas sobre o tema abordado.

2. EVOLUÇÃO HISTÓRICA DE CRIMES DIGITAIS

Desde os primórdios, pode se dizer até mesmo no período do homem primitivo, uma de suas principais funções era construir ferramentas as quais facilitassem seu modo de sobrevivência e atividades diárias, o tempo foi passando o homem evolutivamente foi se modificando físico e mentalmente, e no tocante a criatividade ele mudou tanto na forma de aprimorar suas ferramentas como incrementá-las, tudo para facilitar a vida.

Passando por várias transformações desde revolução agrícola até revolução industrial, as cidades estados começam a se desenvolver, o homem chega no mundo contemporâneo com a chamada revolução tecnológica, aponta-se como ponto forte o processo de globalização, vive-se o mundo informacional, a criação de máquinas bem aprimoradas e pouca mão de obra, não há como negar que a vida ficou mais fácil braçalmente. Entretanto, é imprudente deixar de apontar que todas as revoluções assim como deixaram pontos positivos também deixaram vestígios negativos e, não seria diferente com a revolução tecnológica, em síntese o crime cibernético é apenas um dos pontos negativos que surgiram com o advento da evolução tecnológica.

Desse modo com a evolução de tecnologia, ao se observar o surgimento da internet e até chegar aos primeiros vestígios de crimes informáticos percebe-se que há divergências na doutrina acerca desse tipo de crime, alguns autores apontam com início em 1964, veja:

> A doutrina diverge acerca do primeiro delito informático cometido. Para alguns, o primeiro delito informático teria ocorrido no âmbito do MIT (Massachusetts Institute of Technology), no ano de 1964, onde um aluno de 18 anos teria cometido um ato classificado com cibercrime, tendo sido advertido pelos superiores. Outros ainda referenciam o primeiro caso de que se tem notícia sobre hacking no ano de 1978, na Universidade de Oxford, onde um estudante copiou de uma rede de computadores uma prova. Uma invasão seguida de uma cópia. Até essa data não existia lei sobre crimes informáticos nos Estados Unidos. A Flórida, no mesmo ano, foi o primeiro Estado americano a formular leis sobre informática. Segundo Schjolberg6 (2008, p. 1), muitas pessoas estiveram engajadas no combate ao crime eletrônico no passado. Muitos indicam o americano Donn. B. Parker como um dos primeiros pesquisadores sobre cibercrime, com sua pesquisa, quando consultor de segurança para a Stanford Research Institute. Ele fora o autor do manual para autoridades de aplicação de leis denominado Computer Crime – Criminal Justice Resource Manual, desenvolvido em 1979 e que virou uma “enciclopédia” também para autoridades de fora dos Estados Unidos. Outros autores com grande contribuição na seara são August Bequai e Jay Bloombecker (JESUS, MILAGRE, 2016, 20)

Paralelo a esta informação Tavares e Reis apontam também a década de 70 como sendo o ano que começam a aparecer os primeiros vestígios de crimes cibernéticos, praticados somente por especialistas em informática, pois tinha como objetivo driblar os sistemas de segurança das empresas, com uma visão principalmente das instituições financeiras ou bancárias. Segundo eles hoje um indivíduo não precisa ser mais especialista em informática pois qualquer pessoa com acesso à internet e que possuam conhecimentos informáticos podem praticar crimes digitais, de modo que os usuários domésticos do mundo contemporâneo já possuem esse conhecimento. (TAVARES, REIS, 2014, 33).

Canais de notícias apontam que nesse processo de evolução dos crimes cibernéticos, até Steven Jobs cometeu crime.

> Um bom negócio. Dois jovens californianos, Steven Jobs e Stephen Wosniaz vendem aparelhos chamados blue box para adulterar telefones, de modo que as ligações não fossem cobradas. Em 1976, os dois...
> (SHIMIZU, SETTI, [s.d], online).

No Brasil se teve notícias dos primeiros crimes digitais em meados de 1999, (phishing scam), pescaria de senha, contra bancos. No mesmo ano acontece um caso de grande repercussão envolvendo um empresário e ex-controlador de uma rede de varejo, acusado à época de enviar e-mails, de Londres, com informações falsas, para o mercado financeiro, alardeando a possível quebra de um banco. Daí em diante começa se discutir sobre os crimes informáticos poderem ser praticados de qualquer lugar do mundo e surge então a necessidade de se destacar sobre uma reflexão da importância de criação de leis que tratassem de crimes digitais. (JESUS, MILAGRE, 2016, 21).

Diante disso nota-se que o processo de evolução humana sempre traz modificações no cotidiano dos seres humanos, diante da evolução tecnológica não poderia ser diferente, acessar a internet atualmente torna-se quase que uma necessidade básica, e desse modo todas essas centenas de milhares de pessoas conectadas ao mundo digital, com certeza muitos com poderes aquisitivos enormes, sem falar nas empresas as quais precisam realizar suas atividade diárias, de fato tudo isso chama bastante a atenção dos criminosos cibernéticos.

Diante do exposto conclui-se que como não há ainda uma harmonia entre a doutrina acerca dos marcos históricos de crimes digitais, o que se gerou de certa forma uma instabilidade na criação de leis as quais possam tipificar esse tipo de crime

e, que só agora está podendo ser revisto. No Brasil por exemplo quando começaram surgir os primeiros sinais desses crimes alguns juristas os apontavam como esparsos e que poderiam ser enquadrados nos artigos existentes do Código Penal atual, sem que houvesse a necessidade de criar uma lei específica para os delitos informáticos.

2.1 DADOS SOBRE CRIMES DIGITAIS NO BRASIL

Os dados aqui informados demonstram que em consideravelmente pouco tempo depois de a internet chegar ao Brasil, o país já possuía números alarmantes de criminosos digitais, assim como muitas vítimas também, bem como os enormes prejuízos causados ao mercado financeiro, econômico e social.

O Brasil passou a se preocupar com o crime digital nas últimas duas décadas, estudos e pesquisas apontam que em 2016 o país era o quarto do mundo com maior número de ameaças virtuais.

As pesquisas sempre apontaram para o Brasil na rota dos crimes cibernéticos. Em 2004, de acordo com a Polícia Federal, de cada dez hackers ativos no mundo, oito eram brasileiros. Como se não bastasse, segundo o órgão, à época, aproximadamente dois terços dos crimes envolvendo páginas de pedofilia na internet, detectadas por investigações de agentes brasileiros e no exterior, tiveram origem no Brasil, e mais, as fraudes financeiras envolvendo a internet e correios eletrônicos superava os prejuízos financeiros causados por crimes de assalto a banco. (VASCONCELOS, [s.d], online).

Segundo a corporação da PF os crimes digitais geram mais dinheiro do que o narcotráfico. Segundo dados obtidos pelo CNB – Colégio Notarial do Brasil – O uso da Ata Notarial para comprovação de crimes digitais cresce mais de 582%, nos últimos anos. (CNB, [s.d], online).

À medida em que os computadores e outros meios tecnológicos invadiram o nosso cotidiano os crimes cibernéticos acompanharam esse crescimento, desse modo o computador o smartfone podem ser os agentes facilitadores ou vítimas desse tipo de crime.

> Cada vez mais comuns e abrangentes, os crimes digitais, que vão desde os golpes estelionatários até os casos de violência contra a mulher, representam uma ameaça para os usuários da internet. Prova disso é que nos últimos dois anos, foram registradas mais de 133.732 mil ocorrências de crimes cibernéticos no Brasil. Para fazer prova válida desses crimes perante o Poder

> Judiciário, as vítimas estão utilizando cada vez mais um serviço feito pelos Cartórios de Notas de todo o País: a ata notarial, que nos últimos nove anos cresceu 582% em todo território nacional.
> O Brasil é o segundo país do mundo em casos de crimes cibernéticos, afetando mais de 62 milhões de pessoas, segundo relatório da Norton Cyber Security. Os três tipos de violência digital mais praticadas no país são: ameaça, estelionato e difamação.
> Outros crimes virtuais, como injúria, divulgação de cenas de estupro e de imagens de nudez, sexo ou pornografia, bullying, perseguição digital (stalking), importunação e assédio sexual também são frequentemente notificados e demonstram a vulnerabilidade dos internautas diante dos perigos do mundo digital.
> Neste cenário, a ata notarial tornou-se uma ferramenta segura e cada vez mais procurada para garantir às vítimas respaldo jurídico e proteção diante das ameaças. Documento público, no qual o tabelião, a pedido do interessado, constata fatos e publicações em mídias físicas ou digitais, o ato registra fielmente determinada situação com fé pública, ou seja, com presunção da veracidade, sendo considerada uma prova pré-constituída perante ações levadas ao Poder Judiciário. Dessa forma, pode servir como prova legal de um crime, aceita por qualquer juiz em processos que visem à busca de reparações por dano moral e a exclusão de conteúdos veiculados indevidamente.
> Em números absolutos, as atas notarias no Brasil passaram de 15 mil em 2010, para 90 mil em 2019. Nos três primeiros meses de 2020 os cartórios brasileiros já fizeram 15 mil atas. Entre os exemplos mais utilizados estão as que comprovam crimes em mídias sociais; em mensagens eletrônicas (e-mail) e mensagens instantâneas (WhatsApp, Skype, Snapchat, SMS etc.). (CNB, [s.d], online).

Em 2022, o Brasil foi o segundo país da América Latina mais atingido por ataques cibernéticos, sendo superado apenas pelo México. Os dados foram colhidos pelo FortiGuard labs, laboratório de inteligência e análise de ameaças, da Fortinet, empresa que compõe soluções de cibersegurança (FORTINET, [s.d], online).

> Segundo o levantamento, o País sofreu 103,16 bilhões de tentativas de ataques cibernéticos no ano passado, um aumento de 16% com relação a 2021 (88,5 bilhões de tentativas). O número de tentativas de ataques cibernéticos sofridas pelo País cresceu 61,7% em comparação entre o último trimestre do ano e o anterior. Nos meses de outubro, novembro e dezembro de 2022 foram 30,4 bilhões, contra 18,8 bilhões em julho, agosto e setembro (MEIOEMENSAGEM, [s.d], online).

Conclui-se diante do exposto das pesquisas obtidas, que desde a chegada da internet ao Brasil, os ataques digitais criminosos só crescem e, de 2019 até 2022 os números de crimes cibernéticos atingiram no país números alarmantes, colocando assim no topo, o Brasil como país com o maior número de ataques informáticos no mundo.

2.2 CONCEITO DE CRIMES DIGITAIS

Antes de você entender sobre conceito de crimes digitais é importante destacar que a própria nomenclatura enfrenta complexidade, isso porque algumas doutrinas afirmam que a denominação e classificação relacionada aos atos ilícitos no meio tecnológico são inúmeras: delito informático, delitos cibernéticos, cibercrimes etc. desse modo concluem Fiorillo e Conte (FIORILO, CONTE, 2016, 61), atribuindo a esse tipo de crime como crimes informáticos, segundo os autores essa denominação abarca um campo de estudo maior levando em conta todos os delitos relacionados com o meio digital e as novas tecnologias.

A conceituação atribuída a esse tipo de crime ainda passa por complexidades, ou seja, ainda não existe uma definição pacífica para os crimes praticados no meio virtual, ao passo que se percebe uma doutrina ainda em formação acerca do tema, pois ainda são múltiplas as faces as quais podem ser assumidas pelo meio digital.

A Organização para Cooperação Econômica e Desenvolvimento da Organização Nações Unidas, em 1983, definiu como crime digital, “qualquer conduta ilegal, não ética, ou não autorizada que envolva processamento automático de dados e transmissão de dados”.

Paulo Marco Ferreira Lima atribui aos crimes digitais o conceito de:

> Qualquer conduta humana, comissiva ou omissiva, típica, antijurídica e culpável, em que a máquina computadorizada tenha sido utilizada e, de alguma forma, facilitado de sobremodo a execução ou consumação da figura delituosa, ainda que cause um prejuízo a pessoas sem que necessariamente se beneficie o autor ou que, pelo contrário, produza um benefício ilícito a seu autor, embora não prejudique a vítima de forma direta ou indireta. (LIMA, 2006, 31)

Seguindo o mesmo pensamento, Claudio Líbano Manzur. Professor, Advogado e Secretário Executivo Diretor da Associação de Direito e Tecnologia da Informação do Chile, define os crimes digitais como:

> todas aquelas ações ou omissões típicas, ilegais e maliciosas, sejam atos isolados ou uma série deles, cometidos contra pessoas singulares ou coletivas, realizados através de um sistema de processamento de informação e destinados a causar danos à vítima por meio de ataques à informática saudável, que geralmente produzirão danos colaterais a diversos valores jurídicos, reportando muitas vezes um benefício ilícito ao agente, seja de natureza financeira ou não, agindo com ou sem fins lucrativos. (MANZUR, [s.d], online).

Compreende-se desse modo, que crimes digitais são todos aqueles ilícitos praticados por meio da internet ou que contem com o auxílio desta, gerando danos para a vítima.

Isto posto, conclui-se que dentro do conceito vasto de crimes digitais, se encontram abrangidas as situações em que são utilizadas o computador ou outros dispositivos para a execução de ilícito penal. Assim como as práticas criminosas contra o computador ou em relação as informações que estão inseridas na máquina. Com isso é possível apontar algumas classificações dos crimes cibernéticos em Puros, Mistos e Comuns. Dentre as muitas existentes.

Nesse sentido, nos explica Reginaldo César Pinheiro (PINHEIRO, 2001, 18), que o crime digital puro, abrange todo e qualquer comportamento criminoso que tenha por foco exclusivo o sistema de computador, por atentado físico ou técnico à máquina e seus componentes, incluindo dados e sistema. Contudo podem ser considerados crimes digitais mistos, aqueles que pelo uso da internet, torna-se uma condição imprescindível para que se possa ser efetivado tal conduta, embora o bem jurídico desejado seja diferente do bem informático. O crime virtual comum é aquele que se utiliza do meio virtual, ou seja, a internet, apenas como uma ferramenta para a prática do crime o qual já está tipificado pelo Código Penal.

Logo, os crimes informáticos puros são aqueles que atacam o sistema digital software (ou programa de computador ou dispositivo), hardware (abrange as partes físicas do computador), dados, sistemas e meios de armazenamento etc. Acerca dos crimes mistos, torna-se necessário que exista um computador, pois sem ele é quase impossível a prática do crime, como por exemplo, retiradas de dinheiro dos bancos, em pequenas quantidades, e que se utiliza varia contas bancárias, ou transações financeiras falsas. Doutro modo tem-se os crimes digitais comuns, já inseridos na lei penal (Código Penal): o estelionato (art.171 do CP), a ameaça (art.147 do CP), os crimes contra a honra (art, 138 a 140 do CP), o homicídio (art. 121 do CP), produção de pornografia infantil (Estatuto da Criança e do Adolescente – ECA – lei 8.069/1990) etc. (FURLANETO, GUIMARÃES, 2003, 69)

André Luiz Pereira Spinieli (SPINIELI, 2018, 2005), também assume posição de que não existe ainda conceito único para os crimes no meio digital, desse modo o autor aponta o seguinte posicionamento:

> Como é cediço, desde a década de 1980, o professor alemão Klaus Tiedemann fazia referência a um conceito de crime informático, relatando que se tratava de alusão a todos os comportamentos ilegais de acordo com a legislação vigente ou que eram socialmente prejudiciais, desde que praticados com o emprego de um equipamento automático de processamento de dados. Logo, o conceito, na concepção do professor germânico, abrange o problema da ameaça à esfera privada do cidadão mediante a acumulação, associação, arquivamento e, principalmente, divulgação irrestrita de dados por meio de computadores.

Ante o exposto, comporta dizer que diante de tantas diversidades de que surgem no meio digital, acerca das condutas criminosas, surgem várias dúvidas e insegurança quanto a aplicabilidade e efetividade das normas existentes.

2.3 MARCO CIVIL DA INTERNET

A lei 12.965 de 2014, conhecida como Marco Civil da Internet, a qual em sua tramitação envolveu grande participação social e até mesmo empresarial e acadêmica, apresenta uma grande conquista do Brasil, nessa nova realidade tecnológica em que o mundo vive. Embora sua nomenclatura traga um aspecto de cunho civil, esta lei consagra um grande avanço na ajuda para identificar os crimes cometidos nos espaços virtuais.

A lei começou a ser tramitada mais precisamente em 2009 pelo Ministério da Justiça em colaboração com vários outros entes, desde o Centro de Tecnologia e Sociedade, até passando por colaborações online, de forma direta e aberta, entretanto somente em 2014 é que esse dispositivo normativo veio a ser promulgado. A lei busca através de princípios e garantias trazer mais segurança aos espectadores que precisam utilizar a internet, ou seja, busca tornar o mundo digital um ambiente menos perigoso. O intuito da lei é buscar manter o equilíbrio entre a transferência de conhecimento e a liberdade de expressão, a exemplo: a previsão da segurança, responsabilizando civilmente os provedores e usuários.

O marco civil da internet é composto por três pilares importantes a serem observados:

> neutralidade de rede, liberdade de expressão e privacidade. Em cada um deles, a Lei foi além da consolidação da jurisprudência já existente, buscando resolver problemas pendentes e fornecer diretrizes para a doutrina e para a atuação dos Tribunais.
>
> O respeito ao princípio da neutralidade de rede na internet veda a discriminação no tráfego de dados na internet em razão de seu conteúdo, origem e destino, serviço, terminal ou aplicação. É um importante instrumento

> no estímulo à inovação na internet, facultando o poder de escolha do usuário, promovendo a concorrência e a liberdade de circulação de dados e informações na rede.
> O segundo pilar do Marco Civil da Internet é o reforço da garantia constitucional da liberdade de expressão no ambiente online, procurando equilibrá-la com a proteção da intimidade, da honra e da imagem das pessoas. Além de tratá-la como fundamento das regras sobre internet, o texto é inovador na disciplina sobre a remoção de conteúdos da internet e sobre a responsabilidade de intermediários, um tema que ainda é objeto de controvérsias judiciais. As regras de não responsabilização de intermediários por atos de terceiros (a não ser pelo descumprimento de ordem judicial) e a preocupação com transparência em caso de retirada de conteúdo reforçam o papel da internet como espaço aberto aos debates públicos.
> Por fim, o Marco Civil da Internet introduz o tem a da proteção de dados pessoais no sistema jurídico brasileiro. A partir da perspectiva de que as pessoas são titulares de seus dados pessoais, estabelece regras sobre o consentimento para tratamento de dados, permite somente coleta de dados relacionados com a finalidade das atividades prestadas, reafirma a necessidade de transparência nas políticas de privacidade, entre outras medidas (LEITE, LEMOS, 2014, 26).

Desse modo o princípio da neutralidade da rede impõe aos provedores de acesso, a obrigação de não restringir o acesso de determinados sites e aplicações aos usuários, também sendo proibido aos provedores de acesso fazerem controle de velocidade ou dificultar o acesso a aplicações específicas. Comporta apontar que esse princípio também busca impedir que taxas diferenciadas sejam cobradas dos usuários para que possam acessar a determinados conteúdos e aplicações, sendo livre cobrar tarifas diferenciadas de acordo com a velocidade do acesso ou bagagem de banda utilizada. Os provedores devem observar a todo momento a transparência e razoabilidade a respeito de seus padrões técnicos de administração de tráfego. (LEITE, LEMOS, 2014, 166)

Todavia haverá momentos em que esse princípio poderá ser suprimido, nos casos em que se tratar de requisito indispensável à prestação do serviço, ou em caso de prioridade para serviço de emergência, nessas hipóteses as operadoras as quais fizerem este tipo de tratamento ao usuário, deverá abster-se de lhe causar danos, observando a proporcionalidade, transparência e autonomia informando com antecedência ao usuário (VALENTE, [s.d], online).

A cerca da liberdade de expressão José Luiz Quadros de Magalhães (MAGALHÃES, 2008, 74) aponta:

> Mais do que um direito, a liberdade de expressão pode ser entendida como um conjunto de direitos relacionados às liberdades de comunicação. Sendo diversas as formas de expressão humana, o direito de expressar-se livremente reúne diferentes “liberdades fundamentais que devem ser

> asseguradas conjuntamente para se garantir a liberdade de expressão no seu sentido total".

Esse conjunto de direito visa preservar o direito daqueles que recebem e emitem informações, críticas e opiniões (TÔRRES, 2013, 62).

> "Nesses termos, para a doutrina dominante, falar em direito de expressão ou de pensamento não é falar em direito absoluto de dizer tudo aquilo ou fazer tudo aquilo que se quer. De modo lógico-implícito a proteção constitucional não se estende à ação violenta. Nesse sentido, para a corrente majoritária de viés axiológico, a liberdade de manifestação é limitada por outros direitos e garantias fundamentais como a vida, a integridade física, a liberdade de locomoção. Assim sendo, embora haja liberdade de manifestação, essa não pode ser usada para manifestação que venham a desenvolver atividades ou práticas ilícitas (antissemitismo, apologia ao crime etc.)" (FERNANDES, 2011, 279).

No tocante à proteção dos registros de dados pessoais e das comunicações a lei, as quais estão elencadas no marco civil da internet, determina que os provedores de conexão ou aplicação preservem a intimidade, a vida privada, a honra e a imagem das partes envolvidas, seja diretamente ou indiretamente. Sobe pena de aplicação de sanções penais, civis ou administrativas, de acordo com a proporção da infração.

E importante destacar que os conteúdos de terceiros que causem danos, não trarão responsabilidade civil para o provedor, a não ser que seja constatado descumprimento de ordem judicial, na qual o provedor deveria ter tomado as devidas providencias dentro do prazo estabelecido.

Ainda sobre o princípio da privacidade torna-se necessário apontar os artigos 11, § 1º, 13 caput e 15 caput, da lei 12.965/2014:

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros
> § 1º O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.
> Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.
> Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

Diante de tudo que foi exposto sobre o princípio da privacidade de dados é importante mencionar que a obtenção dos registros de dados, tornam-se também bastante interessante para desvendar certos crimes, no processo de investigação.

O Brasil ainda precisa avançar bastante em tramitações de dispositivos normativos para o combate aos crimes digitais, é notório que as práticas criminosas no meio virtual evoluem com muita rapidez tomando proporções alarmantes, nesse sentido em breve o país deverá passar por várias modificações e implementações de leis para a segurança da informática.

3. CONDUTAS INFORMÁTICAS CONSIDERADAS CRIMISOSAS

Neste capítulo você entenderá que diante do processo de globalização, com a evolução tecnológica e posteriormente o surgimento da internet, a sociedade incorporou um novo modo de elaborar suas atividades diárias, facilitando a vida dos indivíduos em grande escala, nos dias atuais e difícil se deparar com alguém sem que não esteja portando algum tipo de dispositivo tecnológico, o acesso à internet está em quase todas as residências do país e do mundo, até mesmo naqueles lugares considerados como de difícil acesso. Entretanto toda essa revolução por qual a sociedade contemporânea vem passando faz com que surjam as condutas desvantajosas, que são consideradas como criminosas no meio ambiente virtual.

Desse modo o que se pode compreender como condutas criminosas são os comportamentos relacionados a potenciais crimes próprios, em que a informática é o bem jurídico agredido, individuo age diante da internet para praticar crimes de cunho relacionado ao meio digital e aos dispositivos. Importante destacar que as condutas podem ou não ser caracterizadas com crimes, isso vai depender da legislação de cada país (JESUS, MILAGRE, 2016, 41).

Nesse sentido:

> O Brasil precisa enfrentar suas vulnerabilidades cibernéticas. Isso exige um diálogo mais honesto e público sobre as dimensões das ameaças *online* e a importância da higiene digital. No mínimo, os brasileiros precisariam tomar mais precauções para proteger seus dispositivos móveis e reduzir os riscos nas redes sociais. Os bancos e outras instituições financeiras precisam ser mais transparentes em relação a suas respostas aos crimes cibernéticos e à proteção dos dados de seus clientes. O governo, por sua vez, precisa garantir que a legislação nacional para evitar e combater cibercrimes acompanhe o ritmo dos avanços tecnológicos. Apesar da promessa do novo Marco Civil da Internet, as leis atuais são lamentavelmente inadequadas para combater as ameaças existentes. O Brasil precisa de um plano nacional de segurança cibernética e deveria criar um órgão oficial para orientar sua estratégia nacional sobre o tema. Está na hora de os legisladores brasileiros começarem a levar a sério o crime cibernético (MUGGAH, [s.d], online).

Diante disso reforça-se, que os avanços dos dispositivos normativos para combater os crimes da internet no Brasil, ainda deixam bastante lacunas em suas adaptações e que o caminho mais interessante para progredir na tipificação desses crimes é um olhar mais cuidadoso para o tema, por parte do legislativo e judiciário.

3.1 FRAUDE INFORMATICA

A fraude informática ou falsidade, pode ser caracterizada pela inserção, supressão, alteração ou eliminação intencionalmente e ilegítima de dados informáticos, feitos com a intenção de que sejam autênticos, mas que em verdade não são, e o proposito na maioria das vezes deve ser obter alguma vantagem ou até mesmo danificar o dispositivo (JESUS, MILAGRE, 2016, 44).

Crimes em que a ação criminosa busca a sabotagem ou danificação informática, inclusive aqueles atos praticados contra os suportes materiais da informação, como pen drive com dados, e outros dispositivos de armazenamento, são necessariamente crimes os quais devem ser caracterizados como crime de informática (COSTA, [s.d], online).

Segundo Jesus e Milagre (JESUS, MILAGRE, 2016, 44), o Brasil carece de legislação específica para proteger os atos de falsificação e fraude informática nos bancos de dados privados:

> No Brasil, não temos um tipo específico para tutelar esta conduta em casos de bancos de dados privados (podendo se cogitar do delito de falsidade ideológica – art. 299 do Código Penal). Já no âmbito dos crimes praticados por funcionário público contra a Administração Pública, temos o art. 313-A do Código Penal, inserido pela Lei n. 9.983/2000, que assim define, cominando pena de dois a doze anos de reclusão e multa: inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida, para si ou para outrem, ou para causar dano. Da mesma forma, o art. 313-B do Código Penal pune, com pena de detenção de três meses a dois anos, a conduta de modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente. Já para o particular, que acessa bancos de dados da Administração Pública de forma indevida, tem-se a punição prevista no inciso II do § 1º do art. 325 do Código Penal.

Diante de tudo que foi exposto torna-se importante apresentar o seguinte julgado:

> João é professor de uma Universidade Federal. Ele inseriu seu currículo pessoal na plataforma digital Lattes, mantida pelo CNPq. Ocorre que João colocou que seu regime de trabalho na Universidade era de 40 horas semanais, quando, na verdade, era de apenas 20 horas. Essa inexatidão foi descoberta e João foi denunciado, pelo MPF, pela prática do crime de falsidade ideológica, delito previsto no art. 299 do Código Penal: Art. 299. Omitir, em documento público ou particular, declaração que dele devia constar, ou nele inserir ou fazer inserir declaração falsa ou diversa da que devia ser escrita, com o fim de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante: Pena – reclusão, de um a cinco anos, e multa, se o documento é público, e reclusão de um a três anos, e multa, se o documento é particular. Parágrafo único - Se o agente é funcionário

> público, e comete o crime prevalecendo-se do cargo, ou se a falsificação ou alteração é de assentamento de registro civil, aumenta-se a pena de sexta parte. A denúncia narrou o seguinte: “Conforme restou demonstrado nos autos, JOÃO, de forma livre e consciente, inseriu dados falsos na plataforma Lattes (sistema informático da CAPES), com o objetivo de obter uma melhor avaliação do curso de mestrado da Universidade Federal do XXX, do qual seria o coordenador. No dia 22 de fevereiro de 2010, o denunciado inseriu na plataforma mencionada informação inverídica, afirmando que trabalhava como Professor Adjunto Efetivo da XXX num regime de 40 horas semanais, quando, na verdade, seriam 20 horas. As informações lançadas na plataforma Lattes têm relevância no sentido de subsidiarem a atuação do CNPq - Conselho Nacional de Desenvolvimento Científico e Tecnológico no que diz respeito especialmente à avaliação de cursos que podem se beneficiar dos recursos de programas desenvolvidos pela autarquia. Ao inserir na plataforma informações não condizentes com a verdade no que concerne à carga horária que cumpria como professor da XXX, o denunciado pretendeu ludibriar o CNPq nas avaliações trienais sobre o Programa de Pós-Graduação da universidade. Assim agindo, JOÃO praticou o delito previsto no art. 299 do Código Penal.” O STJ concordou com a tese do MPF? A conduta narrada configura crime? NÃO. Não é típica a conduta de inserir, em currículo Lattes, dado que não condiz com a realidade. Isso não configura falsidade ideológica (art. 299 do CP). STJ. 6ª Turma. RHC 81.451-RJ, Rel. Min. Maria Thereza de Assis Moura, julgado em 22/8/2017 (Info 610).

Conforme vimos acima, o crime de falsidade ideológica consiste em “omitir, em documento público ou particular, declaração que dele devia constar, ou nele inserir ou fazer inserir declaração falsa ou diversa da que devia ser escrita, com o fim de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante”.

> Na situação narrada envolvendo João, não há o objeto material do tipo. Isso porque não há “documento” no qual tenha sido inserida declaração falsa. A plataforma Lattes, como se sabe, é virtual e nela o usuário, após colocar seu "login" e senha, insere as informações desejadas. Não se trata, portanto, de um escrito palpável, ou seja, um papel do mundo real, mas sim de uma página em um sítio eletrônico.Para que seja documento eletrônico, é necessária assinatura digital. Embora possa existir "documento eletrônico", não está ele presente no caso concreto. Isso porque somente pode ser considerado “documento eletrônico” aquele que consta em site que possa ter sua autenticidade aferida por assinatura digital. Nesse sentido, a MP 2.200-2/2001, que instituiu a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), dispõe no seu art. 1º: Art. 1º Fica instituída a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras. No Brasil, a infraestrutura de chaves públicas é de responsabilidade de uma Autarquia Federal, o ITI - Instituto Nacional de Tecnologia da Informação, ligado à Presidência da República. Para que pudesse ser considerado documento eletrônico, a plataforma Lattes teria que ter a sua validade jurídica atestada por meio da assinatura digital. Logo, não se pode ter como documento o currículo inserido na plataforma virtual do Lattes do CNPq, porque desprovido de assinatura digital e, portanto, sem validade jurídica. Currículo Lattes é passível de averiguação e, portanto, não é objeto material de falsidade ideológica. O STJ foi além e disse o seguinte: ainda que o

> currículo Lattes pudesse ser considerado um documento digital válido para fins penais, mesmo assim não teria havido crime. Isso porque, como qualquer currículo, seja clássico (papel escrito) ou digital, o currículo Lattes é passível de averiguação, ou seja, as informações nele contidas deverão ser objeto de aferição por quem nelas tenha interesse. Quando o documento é passível de averiguação, o STJ entende que não há crime de falsidade ideológica, mesmo que o agente tenha inserido nele informações falsas. Nesse sentido: (...) Já se sedimentou na doutrina e na jurisprudência o entendimento de que a petição apresentada em Juízo não caracteriza documento para fins penais, uma vez que não é capaz de produzir prova por si mesma, dependendo de outras verificações para que sua fidelidade seja atestada. (...)
>
> STJ. 5ª Turma. RHC 70.596/MS, Rel. Min. Jorge Mussi, julgado em 01/09/2016. (...) somente se configura o crime de falsidade ideológica se a declaração prestada não estiver sujeita a confirmação pela parte interessada, gozando, portanto, de presunção absoluta de veracidade. (...) STJ. 6ª Turma. RHC 46.569/SP, Rel. Min. Maria Thereza de Assis Moura, julgado em 28/04/2015.

Neste sentindo é a opinião também da doutrina "(...) havendo necessidade de comprovação - objetiva e concomitante -, pela autoridade, da autenticidade da declaração, não se configura o crime, caso ela seja falsa ou, de algum modo, dissociada da realidade." (NUCCI, 2013, p. 1.138)

Portanto, no caso exposto, o STJ entendeu que o currículo Lattes não é considerado um documento eletrônico pois não exige assinatura digital, e por ser passível de averiguação, desse modo o STJ julgou o caso entendendo não haver crime de falsidade ideológica, mesmo que o agente tenha inserido falsas informações.

3.2 INFORMAÇÕES VAZADAS E DADOS ROUBADOS

No espaço virtual lidar com informações e dados de terceiros é algo bastante complexo de se tratar ao se observar como os crimes cibernéticos evoluem rapidamente, pois muitos são os meios que os criminosos encontram para atacar empresas, prestadoras de serviços e pessoas físicas, embora a legislação esteja a todo momento a tipificar as condutas criminosas no espaço digital, muitas vezes os próprios colaboradores da entidade tornam os dados e informações vulneráveis.

Com isso vazamento de informações consiste no ato de coletar e divulgar informações ou dados restritos e importantes através da internet. Com isso as pessoas não autorizadas adquirem os acessos a informações confidenciais as quais não poderiam ser tornadas públicas.

> O vazamento pode ocorrer de diversas maneiras. A primeira delas consiste no uso de malwares que explorem vulnerabilidades no sistema para obter acesso à informação restrita. A segunda maneira ocorre quando o atacante acessa a conta de um usuário que possui senhas fáceis de se adivinhar, ou cujas credenciais foram vazadas anteriormente. Em terceiro lugar, tem-se o acesso, mediante furto ou descarte inadequado, de equipamentos ou mídias removíveis que contenham os dados em questão. Por fim, o vazamento também pode ocorrer nos casos em que funcionários da própria empresa repassam os dados a terceiros (CERT.BR, 2021, 2).

Esses dados são vazadores por vários motivos, o que ocorre logo em seguida na maioria dos casos é extorsão, furto de identidade, violação a privacidade e aplicação de golpes.

> Nos casos de furto de identidade, os criminosos podem usar os dados vazados para emissão de cartão de crédito, criação de contas bancárias, liberação de empréstimos ou para transferência de bens móveis ou imóveis, com potencial para causar um prejuízo financeiro considerável para a vítima. Nos casos de violação de privacidade, os criminosos expõem, em páginas da internet, dados íntimos da vítima, como conversas privadas, dados médicos ou fotos sensuais. Já no caso de extorsão, os criminosos chantageiam as vítimas exigindo dinheiro para que seus dados não sejam publicamente expostos. Um dos casos de ciberataque que ganhou destaque na mídia em 2021 foi o vazamento de dados da empresa americana Facebook. Os dados vazados consistiram nas informações pessoais de mais de 533 milhões de usuários da rede social, provenientes de 106 países diferentes. Entre as informações vazadas, constam o telefone celular, nome de usuário, nome completo, localidade, data de nascimento e, em alguns casos, o endereço eletrônico20. Os dados foram expostos de forma gratuita em um fórum da comunidade hacker.(ANTUNES, 2022, 46)

Entre as principais técnicas de invasão a dados e informações destacam-se: ransomware, spywares e phishing. Ransomware basicamente é o sequestro dos dados feito através da instalação de um software que captura os dados importantes do computador ou sistema. Pode ser em todo o disco rígido ou em uma parte específica. Quando os dados são capturados tornam-se criptografados e só podem ser acessados através de senha, no momento em que isso acontece logo em seguida o sequestrador solicita o pagamento de resgate.

Spyware, são softwares de espionagem, podem capturar telas e até gravar trechos inteiros de uma utilização, e até mesmo tomar acesso a dispositivos do computador. Muistos são os casos que acontecem sobre o acesso dos criminosos a câmeras e microfones de dispositivos para fazerem capturas de interações que

acontecem próximo ao dispositivo e desse modo possivelmente no futuro obter vantagens.

O phishing, normalmente consiste em técnicas criativas de induzir a vítima ao erro, acreditando esta que está fazendo uma coisa e na verdade está fazendo é outra a qual está beneficiando o próprio golpista. A exemplos podem ser destacadas as atualizações de senhas, uso de contas de e-mails falsos (GALVÃO; SILVA, [s.d], online).

Com isso, muito importante é saber quais atitudes tomar para se proteger desses tipos de ataques, tão quanto as políticas públicas que protegem os vazamentos de dados, as vezes coisas muito simples aumentam significativamente seu nível de segurança.

Não ofereça seus dados para meios não oficiais, na maioria das vezes se o indivíduo adquire um vínculo com algum tipo de instituição, pode ter em mente que nenhuma delas irá solicitar a senha de acesso por e-mail ou WatSapp, simplesmente por envolver um procedimento de segurança padrão, portanto quando isso acontece é sempre interessante ficar desconfiado.

Prestar atenção nos e-mails recebidos de endereços desconhecidos. Normalmente confirmar com o remetente por um contato conhecido, sobre o recebimento da mensagem, é um ponto importante de se fazer. Downloads de sites desconhecidos não devem ser executados pois na maioria das vezes os conteúdos baixados oferecem riscos, com conteúdos maliciosos. Assim quanto maior for a vigilância menos chances de ataques criminosos no espaço digital.

4. RELAÇÃO ENTRE O DIREITO PENAL E CRIME DIGITAL

Como muito já foi exposto nos capítulos acima, o processo de globalização e o surgimento da internet, trouxeram inúmeras mudanças para o cotidiano das pessoas, o ordenamento jurídico brasileiro ao longo dos anos vem passando por intensas mudanças para alcançar os fatos criminosos que surgem a todo momento no espaço virtual.

Desse modo com o objetivo de proteger o indivíduo dos crimes praticados nesse ambiente, foram adaptados dispositivos normativos, no Brasil, os quais buscaram tipificar crimes informáticos e agravarem determinados crimes, violação de dispositivo digital, furto e estelionato etc. Praticados através da internet. com isso, o Direito Penal assumiu seu papel de regulamentar esses tipos de crimes, cometidos virtualmente. Essa tipificação representa, aparentemente, um esforço do legislador em adequar o Direito brasileiro à realidade da era da informatização advinda do processo de globalização.

> Nessa perspectiva, e considerando a diversidade de tipificações e as penas brandas, a hipótese definida consiste na ideia de que a legislação não se mostra suficiente, haja vista que o rol de crimes disciplinados pela lei está distante de compreender a realidade prática desse tipo de delito. Ademais, a maior evidência da insuficiência da legislação está disposta na parte das punições, que não se mostram com a força necessária para assumir o papel preventivo e sancionador. (FREITAS, SANTOS, CURY, [s.d], online).

Portanto a constante inovação, possui dinâmica total, ao passo que responde à conduta social de determinada sociedade frente à internet. Notoriamente olhando para o passado não tão distante podia se perceber que em hipótese alguma seria possível a prática de bullying a distância, a não ser pessoalmente. Atualmente esta prática tornou-se super comum, são muitos acessos a redes sociais, como WhatsApp, Facebook, Instagram, as redes sociais são portas em que a todo momento dão acesso aos indivíduos conectados, a várias culturas e pensamentos diferentes, e o fato e que muitos não conseguem lidar com esse tipo de meio virtual.

> Sabe-se que a polícia civil, hoje a responsável pelas investigações de crimes no Brasil, enfrenta dificuldades estruturais, financeiras e técnicas para a resolução dos crimes, dos mais “comuns” aos mais difíceis. Com o advento da modalidade de crimes na área virtual, o não solucionamento dos casos é ainda maior, dado a internet ser de fácil acesso a todos e de haver pouquíssimas necessidades de identificação. Waldek Fachinelli Cavalcante preconiza “Alguns passos vão sendo dados no caso brasileiro, contudo, ainda

> tímidos diante da expansão da internet" (2015, p.19). Assim, não estão, por diversos motivos, os órgãos judiciários e investigativos preparados para essa nova criminalidade (HORITA; MORAIS; OLIVEIRA, 2021, 07).

Assim sendo, pode se concluir que o direito penal brasileiro muito precisa progredir diante das evoluções criminosas no mundo virtual, pois ao se observar como os crimes cibernéticos são abordados no Brasil, constata-se que realmente ainda não existe dispositivos que foram criados especificamente para tratar dos crimes digitais, somente os legisladores tentam qualificar fatos ilícitos que ocorrem ao código penal atual, com isso não significa que estejam sendo arbitrários, entretanto o que ocorre pelo que se percebe, é que muitas lacunas vão surgindo, e de certa forma algumas condutas criminosas no espaço virtual as vezes acabam ficando sem punição.

4.1 INVESTIGAÇÃO DOS CRIMES CIBERNÉTICOS

A investigação dos crimes digitais no Brasil, notoriamente sempre foi um desafio, a falta de punição aos criminosos que praticam delitos na internet sempre encontra como aliada a demora na apuração do delito e a identificação de autoria em consequência do tempo percorrido entre a consumação do crime e a sua apuração na fase de investigação.

> A demora na apuração dos crimes virtuais pode gerar impunidade dos infratores. Isso porque no caso de crimes de menor potencial ofensivo, como é o exemplo dos crimes contra a honra e crime de invasão de dispositivo informático, existe grande chance de o crime prescrever antes mesmo de entrar em um efetivo processo contra o praticante do crime. Isso ocorre porque as penas previstas para esses crimes são baixas (até dois anos), o que significa que é muito fácil ocorrer prescrição retroativa pela pena aplicada em concreto (CAVALCANTE, [s.d], online).

Os criminosos do ambiente digital ao que se percebe, ao longo de toda evolução tecnológica, é que conseguem se articular de forma bastante organizada, muitas vezes são organizações criminosas que abrangem todo o Brasil e ainda possuem membros atuando fora do país, com isso eles constroem esquemas bem articulados de ataques criminosos no espaço virtual, tornando assim mais difícil a vida das autoridades policiais na investigação dos delitos.

Por outro lado, não é o que se percebe dos órgãos de investigação de cada Estado:

> diferentemente dos criminosos, nota-se que não há uma integração entre os órgãos de investigação de cada Estado, e a maioria das delegacias carecem em profissionais especializados em crimes virtuais, o que revela a importância da capacitação de profissionais da área criminal que poderiam ser trazidos, por meio de políticas públicas nacionais voltadas aos órgãos de segurança pública e estimular o investimento por parte dos Estados nessa área tão importante (WENDT e JORGE, 2013, 238).
> Por vezes, a polícia se depara com quadrilhas especializadas na prática de crimes virtuais, sendo que cada membro reside em um Estado diferente. Exemplo disso foi um dos casos apresentados no programa “Profissão Repórter”, em que havia 20 pessoas envolvidas em diversas práticas criminosas, como transferências fraudulentas de contas, pagamento de boletos e compras na internet com cartões clonados. É evidente que houve nesse caso uma integração de criminosos de diversas localidades, sendo que o líder residia no estado do Pará, enquanto o segundo na linha de comando residia em Goiás (GLOBO, [s.d], online).

Nas investigações sobre crimes virtuais nada muda acerca da exigência da materialidade das provas, as quais devem ser obtidas de forma lícita, sob pena de não poderem ser utilizadas na comprovação da prática do crime. Certamente nesse contexto nada mudou conforme quais modos devem ser seguidos pelos profissionais de segurança, não que se exija mudanças do modo como as provas ou investigações devam seguir, entretanto, o que se espera é que novas ideias e ferramentas e políticas para investigação desses tipos de crimes sejam criadas.

Assim aponta Jorge:

> A investigação criminal tecnológica é o conjunto de recursos e procedimentos, baseados na utilização da tecnologia, que possuem o intuito de proporcionar uma maior eficácia na investigação criminal, principalmente por intermédio da inteligência cibernética; extração de dados de dispositivos eletrônicos; novas (e velhas) modalidades de afastamento de sigilo; utilização de fontes abertas; equipamentos e softwares específicos que permitem a análise de grande volume de dados; identificação de vínculos entre alvos; obtenção de informações impossíveis de serem agregadas de outra forma (2020, p. 17).

Você percebeu que para que sejam efetivas as investigações dos crimes digitais no Brasil, algumas melhorias no ordenamento jurídico precisam acontecer, desde agilidade na apuração das provas que levam ao criminoso, utilizar os próprios meios tecnológicos para o auxílio nas investigações e uma maior capacitação de profissionais para a área da segurança cibernética.

Diante do exposto conclui-se que nenhum ato normativo para qualificar esse tipo de procedimento até agora foi criado e com certeza nos próximos anos o Brasil criará leis para qualificar os crimes na internet. Desse modo deixará de certa forma de adotar a política de adaptar as leis já existentes para os atos ilícitos que vem surgindo

no mundo virtual, e o que se espera é que espera é que grandes mudanças positivas surgiram para a segurança da internet no Brasil.

4.2 JULGADOS SOBRE CRIMES DIGITAIS

A jurisprudência se consolida através do termo jurídico, que significa o conjunto das decisões, aplicações e interpretações das leis. Nesse sentido ela pode ser compreendida de três formas, como a decisão isolada de um tribunal que não tem mais recursos, pode ser um conjunto de decisões reiteradas dos tribunais, ou as súmulas de jurisprudência, que são as orientações resultantes de um conjunto de decisões proferidas com mesmo entendimento sobre determinada matéria. Desse modo torna-se necessário abordar alguns julgados para conjugar com os apontamentos supracitados sobre o tema.

Autoridades judiciarias brasileiras podem requisitar dados diretamente a provedores que se encontram fora do território nacional, de acordo com o artigo 11 do Marco Civil da Internet (lei 12.965/ 2014),e do art. 18 da Convenção de Budapeste.

> O caso concreto:
>
> A Federação das Associações das Empresas de Tecnologia da Informação (Assespro Nacional) ajuizou ação declaratória de constitucionalidade (ADC) pedindo para que o STF declarasse constitucionais os seguintes dispositivos:
>
> a) Decreto Federal nº 3.810/2001, que promulgou o Acordo de Assistência Judiciário-penal firmado entre o Brasil e os Estados Unidos (Mutual Legal Assistance Treaty – "MLAT");
>
> O que é o MLAT?
>
> Em inglês, MLAT significa "Mutual Legal Assistance Treaty" e consiste em um acordo bilateral por meio do qual os EUA e o Brasil se comprometem a prestar auxílio jurídico direto em matéria processual.
>
> O MLAT foi a forma encontrada para desburocratizar e tornar mais célere e fácil a cooperação jurídica internacional, que antes era feita apenas por meio de cartas rogatórias que, no entanto, são caras e demoradas.
>
> As cartas rogatórias demoram mais para serem cumpridas porque exigem maiores formalidades e, para serem enviadas e recebidas, precisam passar pelos canais diplomáticos de cada país. No Brasil, para serem cumpridas, precisam ainda da autorização do STJ.
>
> O MLAT, por sua vez, é um instrumento de Auxílio Direto, permitindo que o pedido de auxílio seja formulado diretamente pelo juiz de 1ª instância, sendo desnecessário o juízo prévio de delibação do STJ. A tramitação desses pedidos é coordenada pela Autoridade Central brasileira designada em cada tratado firmado, conforme explica o Manual de Cooperação Jurídica Internacional do Ministério da Justiça editado em 2012 (www.portal.mj.gov.br).

O MLAT entre o Brasil e os EUA foi assinado em 1997, mas promulgado apenas em 2001, por meio do Decreto nº 3.810/2001.

Por meio desse acordo, as partes (Brasil e EUA) se obrigam a prestar assistência mútua, em matéria de investigação, inquérito, ação penal, prevenção de crimes e processos relacionados a delitos de natureza criminal.

A assistência incluirá: a) tomada de depoimentos ou declarações de pessoas; b) fornecimento de documentos, registros e bens; c) localização ou identificação de pessoas (físicas ou jurídicas) ou bens; d) entrega de documentos; e) transferência de pessoas sob custódia para prestar depoimento ou outros fins; f) execução de pedidos de busca e apreensão; g) assistência em procedimentos relacionados a imobilização e confisco de bens, restituição, cobrança de multas; e h) qualquer outra forma de assistência não proibida pelas leis do Estado Requerido.

Os EUA mantêm acordos semelhantes com diversos outros países do mundo.

b) o art. 237, II, do CPC/2015:

Art. 237. Será expedida carta:

(...)

II - Rogatória, para que órgão jurisdicional estrangeiro pratique ato de cooperação jurídica internacional, relativo a processo em curso perante órgão jurisdicional brasileiro;

c) os arts. 780 e 783 do CPP:

Art. 780. Sem prejuízo de convenções ou tratados, aplicar-se-á o disposto neste Título à homologação de sentenças penais estrangeiras e à expedição e ao cumprimento de cartas rogatórias para citações, inquirições e outras diligências necessárias à instrução de processo penal.

Art. 783. As cartas rogatórias serão, pelo respectivo juiz, remetidas ao Ministro da Justiça, a fim de ser pedido o seu cumprimento, por via diplomática, às autoridades estrangeiras competentes.

De acordo com a requerente, o procedimento do MLAT e das cartas rogatórias têm sido adotados como regra pelos juízes e Tribunais brasileiros. Assim, quando o Poder Judiciário nacional precisa de um dado ou documento que se encontra em posse de empresas sediadas em outros países, em regra, ele se vale do MLAT ou da carta rogatória. Por outro lado, quando os juízes e Tribunais brasileiros querem um dado ou informação de empresas de tecnologia internacionais, eles têm feito requisições diretas para essas empresas sem adotar o MLAT ou a carta rogatória.

Para a autora, ao fazer isso, é como se o Poder Judiciário estivesse fazendo uma declaração escamoteada de inconstitucionalidade desses dispositivos acima transcritos porque eles não são respeitados.

Em suma, estaria ocorrendo o afastamento ou a não aplicação desses atos normativos em relação às empresas de tecnologia.

Veja um caso concreto que demonstra como o Poder Judiciário brasileiro faz essa requisição direta (prática condenada pela associação autora):

V.N., professor de um colégio, estava sendo investigado pela Polícia, suspeito de praticar assédio sexual contra suas alunas. Esse assédio seria praticado principalmente por meio das redes sociais Facebook e Instagram.

O juiz, a partir de representação da autoridade policial, determinou que à Facebook Inc., sediada nos EUA, fornecesse o conteúdo das mensagens privadas enviadas pelo professor nas duas redes sociais.

A empresa impetrou mandado de segurança contra essa determinação judicial afirmando que o fornecimento do material dependeria de procedimento de cooperação internacional (MLAT ou carta rogatória, na forma do Decreto nº 3.810/2001 ou dos arts. 780 e 783 do CPP).

O Tribunal de 2ª instância denegou a segurança pleiteada, razão pela qual a Facebook Inc. interpôs recurso ordinário ao STJ. No recurso, insistiu na necessidade de utilização da cooperação jurídica internacional para obtenção dos dados eletrônicos solicitados e pediu o afastamento da multa.

O STJ deu provimento ao recurso da empresa Facebook?

Não. O STJ afirmou que o fato de a recorrente estar sediada nos Estados Unidos não tem o condão de eximi-la do cumprimento das leis e decisões judiciais brasileiras, uma vez que disponibiliza seus serviços para milhões de usuários que se encontram em território nacional.

O art. 11 da Lei nº 12.965/2014 (Marco Civil da Internet) é claro na determinação de aplicação da legislação brasileira a operações de coleta, armazenamento, guarda e tratamento de dados por provedores de aplicações, exigindo apenas que um desses atos ocorra em território nacional:

Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

O que se espera de empresas que prestam serviço no Brasil é o fiel cumprimento da legislação pátria e cooperação na elucidação de condutas ilícitas, especialmente quando regularmente quebrado por decisão judicial o sigilo de dados dos envolvidos.

O armazenamento em nuvem, estrategicamente utilizado por diversas empresas nacionais e estrangeiras, possibilita que armazenem dados em todos os cantos do globo, sem que essa faculdade ou estratégia empresarial possa interferir na obrigação de entregá-los às autoridades judiciais brasileiras quando envolvam a prática de crime em território nacional.

A recalcitrância injustificada atrai a imposição de multa como penalização da prática de ato atentatório à dignidade da Justiça. Seu valor deve ser proporcional à capacidade da parte renitente, sob pena de enfraquecimento desse instrumento de coerção.

A multa fixada pelo magistrado no caso concreto atende aos requisitos indicados, não havendo falar em excesso, já que a capacidade financeira da recorrente é notoriamente gigantesca. O valor diário da multa imposta foi aplicado de forma escalonada, chegando ao limite de R$ 50 mil, apenas alcançado pela resistência obstinada da destinatária à determinação judicial. Esse valor se revela razoável e proporcional à gravidade da conduta omissiva praticada com absoluto desrespeito e desprestígio ao Poder Judiciário. Em verdade, trata-se do único instrumento legítimo à disposição do magistrado, que está, segundo a teoria dos poderes implícitos, autorizado a utilizar os meios necessários para o exercício de sua competência jurisdicional.

> Eventual diminuição nos valores apenas contribuirá para a perpetuação da recalcitrância que pratica contra decisões judiciais, situação repetida em inúmeros processos em andamento.
>
> Quanto à alegada necessidade de utilização de pedido de cooperação jurídica internacional, o mecanismo é necessário apenas quando haja necessidade de coleta de prova produzida em jurisdição estrangeira, não quando seu armazenamento posterior se dê em local diverso do de sua produção por opção da empresa que preste serviços a usuários brasileiros (STJ. Corte Especial. Inq 784/DF, Rel. Min. Laurita Vaz, DJe de 28/8/2013).
>
> Em suma:
>
> Empresas que prestam serviços de aplicação na internet em território brasileiro devem necessariamente se submeter ao ordenamento jurídico pátrio, independentemente da circunstância de possuírem filiais no Brasil e/ou realizarem armazenamento em nuvem.
>
> STJ. 5ª Turma. RMS 66.392-RS, Rel. Min. João Otávio de Noronha, julgado em 16/08/2022 (Info 750).

Percebe-se diante do caso exposto, que mesmo o art. 11 do marco civil da internet possuindo respaldo junto à convenção de Budapeste, ainda sim a requerente se viu no direito de questionar sobre a constitucionalidade de obrigação das autoridades judiciarias brasileiras seguirem o acordo de Assistência Judiciário-penal, firmado entre Brasil e EUA. Entretanto o STJ, cuidou para que sua decisão fosse mantida apontando de forma objetiva as razoes pelas quais não entenderia o julgamento de forma diferente, entende-se que quando determinada empresa estrangeira decide atuar no território nacional brasileiro prestando serviço de aplicação, deverá respeitar e observar as leis especificas brasileira.

O segundo julgado, trata-se de um crime envolvendo pornografia infantil, armazenamento e disseminação do conteúdo pornográfico através de computador e smartfone.

> Caso concreto julgado pelo STJ (REsp 1970216- SP):
>
> R.F.P utilizava o dispositivo Dreamule, uma nova versão do Emule, aplicativo utilizado para baixar arquivos de música, vídeos e fotos que são compartilhados entre os próprios usuários.
>
> Em investigação realizada pela Polícia Federal ficou constatado que R.F.P era um dos usuários que baixava e compartilhava arquivos de pornografia infantil.
>
> Foi realizada a busca e apreensão na sua residência tendo sido constatado que ele compartilhou mais de 30 arquivos envolvendo crianças e adolescentes no dispositivo Dreamulee que também mantinha armazenado em seu notebook aproximadamente 20 arquivos de pornografia infantil.
>
> R.F.P. foi denunciado pelo Ministério Público Federal pela prática dos delitos previstos nos arts. 241-A e 241-B do ECA, em concurso material.
>
> A defesa pediu par que o delito do art. 241-B do ECA (armazenamento) fosse absorvida pelo crime do art. 241-A do ECA (distribuição). Para o réu, a

> conduta de armazenar é menos grave, sendo utilizada como meio para o compartilhamento dos arquivos.
>
> O STJ não concordou com os argumentos da defesa.
>
> É pacífica a jurisprudência no sentido da autonomia dos tipos penais trazidos nos arts.241-A e 241-B, ambos do ECA, uma vez que o crime noart. 241-B não configura fase normal nem meio de execução para o crime do art. 241-A.
>
> É possível que alguém compartilhe sem armazenar, como pode realizar o armazenamento sem a transmissão. Ou seja, são efetivamente verbos e condutas distintas, que têm aplicação autônoma.
>
> Com efeito, é plenamente admissível que uma pessoa, navegando na internet, encontre conteúdo pornográfico infantojuvenil e o repasse para outros, praticando a conduta “disponibilizar” sem, contudo, armazenar tal conteúdo em seus dispositivos eletrônicos. De outro lado, é indiscutível que eventual conteúdo pornográfico da mesma natureza pode ser armazenado em dispositivo (pen drive, HD, CD etc.) ou nuvem, sem jamais vir a ser compartilhado ou divulgado. Com isso em mente, é forçoso reconhecer a autonomia de cada uma das condutas apta a configurar o concurso material, afastando-se a aplicação do princípio da consunção.
>
> Reforça esse entendimento o fato de que, não raras vezes, evidencia-se diferença entre o conteúdo dos arquivos/dados armazenados e o conteúdo daqueles divulgados e/ou a ausência de correspondência entre a quantidade armazenada e a quantidade compartilhada, o que denota a autonomia de cada conduta.
>
> Da mesma forma, a constatação de que o armazenamento ocorreu após a divulgação/compartilhamento de arquivos de imagens/vídeos contendo pornografia infantojuvenil e/ou cenas de sexo envolvendo crianças e adolescentes impede se cogite da aplicação do princípio da consunção entre as condutas:
>
> O STJ compreende que o armazenamento de imagens e/ou arquivos de pornografia e a posterior transmissão parcial destes caracterizam condutas autônomas.
>
> O acórdão recorrido estabeleceu que os arquivos armazenados tinham conteúdo diferente daqueles disponibilizados em momento anterior.
>
> STJ. 6ª Turma. AgRg no REsp n. 1.847.460/SP, relator Ministro Rogerio Schietti Cruz, julgado em 14/3/2023.

No julgado exposto fica claro mais uma vez o poder judiciário fazendo suas adaptações ao caso concreto, buscando o entendimento para adequar ao Estatuto da Criança e do Adolescente, os crimes praticados com o auxílio da internet.

O julgado a seguir aponta a inadmissibilidade das provas digitais sem registro documental acerca dos procedimentos adotados pela polícia para a preservação da integridade, confiabilidade e autenticidade dos elementos informáticos.

> Caso adaptado: a Polícia Civil realizou operação para investigar e prender uma suposta organização criminosa de hackers que teria furtado dinheiro de correntistas de bancos. João foi um dos indivíduos preso e denunciado pelo

> Ministério Público por furto, organização criminosa e lavagem de dinheiro. A defesa de João impetrou habeas corpus argumentando que a imputação dos crimes está fundamentada em supostas provas digitais em relação às quais houve quebra da cadeia de custódia. As provas existentes contra João foram extraídas dos computadores apreendidos na sua residência, no entanto, não houve registro documental dos procedimentos adotados pela polícia para a preservação da integridade, autenticidade e confiabilidade dos elementos informáticos.
> Logo, houve quebra da cadeia de custódia (art. 158-A e seguintes do CPP). O STJ concordou. Não há como assegurar que os elementos informáticos periciados pela polícia são íntegros e idênticos aos que existiam nos computadores do réu, o que acarreta ofensa ao art. 158 do CPP com a quebra da cadeia de custódia dos computadores apreendidos pela polícia, inadmitindo-se as provas obtidas por falharem num teste de confiabilidade mínima.
> STJ. 5ª Turma. RHC 143169/RJ, Rel. Min. Messod Azulay Neto, Rel. Acd. Min. Ribeiro Dantas, julgado em 7/2/2023 (Info 763).

O julgado supracitado aponta como procedimento crucial às provas, o registro documental, com isso a defesa do acusado afirma que houve a quebra da cadeia de custódia, desse modo a defesa pediu a inadmissibilidade da prova extraída dos computadores, e o STJ concordou.

O que se pode extrair do exposto é que houve imaturidade ou despreparo por parte das autoridades policiais. Mais uma vez o ordenamento jurídico brasileiro se demonstra inseguro tanto na qualificação dos profissionais como nos dispositivos normativos os quais se referem ao direito digital.

5. CONSIDERAÇÕES FINAIS

O Surgimento da tecnologia acelerou e continua acelerando em grande proporção o processo de globalização, os avanços computacionais fizeram modificações sem precedentes no cotidiano da humanidade, hoje pode-se dizer que a tecnologia atua de forma vital sobre o desenvolvimento econômico, cientifica e social além de outras áreas também.

E grande a competição em todos os cenários econômicos mundiais e internamente nos países, com isso a informação precisa e ágil torna-se um dos pontos mais importante a ser buscado por aqueles que buscam crescimento, seja de forma pessoal, empresarial, cientifica etc. Justamente é nesse sentido que o uso da internet se tornou no mundo contemporâneo uma necessidade básica, onde as pessoas buscam inúmeras ferramentas para darem destaques, precisão e agilidades em suas atividades, de certa forma se sentem seguras e entendem que esse mundo virtual de grandes novidades impacta positivamente suas vidas de forma significativa.

Com isso, diante de toda a exposição da sociedade ao meio cibernético surgem as novas formas de criminalidade, as quais assolam a todos os que se encontram inseridos nesse meio. São inúmeras as formas de cometimento de crimes no espaço virtual. Crimes os quais diante das pesquisas ainda nem possuem definições únicas, pois mesmo sendo algo que não é mais considerado como novidade no mundo moderno, ainda sim, a internet cria infindáveis contextos dentre os quais são praticados os crimes informáticos.

O ordenamento jurídico brasileiro segue buscando criar leis que tipifiquem os crimes informáticos, uma das mais recentes foi a Lei 14.155/2021 que estabelece pena aos crimes no ambiente digital, dentre eles a violação de dispositivos informáticos, o furto e o estelionato cometidos pela internet ou por meio de dispositivos eletrônicos. Mas ainda sim são inúmeras a vacâncias e que muitas vezes geram impunidades para os criminosos do mundo digital. Sem sombra de dúvidas se confirma os impactos negativos significativamente na sociedade, acerca desses crimes. Portanto conclui-se que por enquanto o déficit de leis para combater os crimes virtuais no Brasil ainda causa bastante impacto negativo na vida social, o processo de investigação sobre os crimes cibernéticos inda é muito lento e não gera a eficiência que se espera, ainda são precárias as regulamentações e geram fragilidade nas estruturas das instituições penais.

6. REFERÊNCIAS

ANTUNES, Priscila Lucas. Da tipificação penal dos ataques cibernéticos no contexto da sociedade de risco: uma abordagem a partir da convenção de Budapeste. Disponível em: https://repositorio.ufsc.br/bitstream/handle/123456789/232487/TCC_PRISCILA_ANTUNES_VERS%C3%83O_FINAL.pdf?sequence=1. Acesso em 07/11/2023

AFREITAS, Victor Valério Medeiros Siqueira. Crimes virtuais: um olhar sob a ótica do direito penal. Revista Ibero. Disponível em: https://periodicorease.pro.br/rease/search. Acesso em 08/11/2023

https://www.buscadordizerodireito.com.br/jurisprudencia/detalhes/e2e2fd34c1cfebdf431177db8e49fdd2?palavra-chave=Crimes+Inform%C3%A1ticos&criterio-pesquisa=e&forma-exibicao=apenas-com-informativo&ordenacao=data-julgado. Acesso em: 10/11/2023

https://www.buscadordizerodireito.com.br/jurisprudencia/detalhes/09859012c567eb2b02d10dddf624e9d3?palavra-chave=Crimes+Inform%C3%A1ticos&criterio-pesquisa=e&forma-exibicao=apenas-com-informativo&ordenacao=data-julgado. Acesso em 11/11/2023.

https://www.cnbrs.org.br/Noticias/VisualizarNoticia/9307

https://www.cnbrs.org.br/Noticias/VisualizarNoticia/9307
https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2022/fortiguard-labs-relatorio-ciberataques-brasil-2021
https://www.meioemensagem.com.br/proxxima/brasil-ataques-ciberneticos

COSTA, Marco Aurélio Rodrigues da. Crime de informática: introdução e história do computador. Disponível em: https://egov.ufsc.br/portal/sites/default/files/29402-29420-1-pb.pdf. Acesso em 06/11/2023.

CAVALCANTE, Márcio André Lopes. Primeiros comentários à Lei 12.737/2012, que tipifica a invasão de dispositivo informático. 2012. Disponível em: 22. Acesso em: 11/11/2023.

FERNANDES, Bernardo Gonçalves. Curso de direito constitucional. 3. ed. Rio de Janeiro: Lumen Juris, 2011.

FIORILLO, Celso Antônio Pacheco; CONTE, Christiany Pegorari. Crimes no meio ambiente digital e a sociedade da informação. 2 ed. São Paulo Saraiva 2016.

FURLANETO NETO, Mário; GUIMARÃES, José Augusto Chaves. Direito da informática: crimes na Internet: elemento para uma reflexão sobre a ética informacional. Revista do Concelho de Justiça Federal. n 20, mar 2003.

GALVÃO E SILVA. Vazamento e roubo de dados: como acontecem e como se precaver. Disponível em: https://www.galvaoesilva.com/roubo-de-dados/. Acesso em: 07/11/2023.

GLOBO. Profissão Repórter 29 09 2015 - Crimes cometidos pela internet no Brasil. 2015. Disponível em: < http://g1.globo.com/profissao-reporter/noticia/2015/09/profissao-reporter-mostradiferentes-crimes-cometidos-pela-internet.html>. Acesso em: 17 mai. 2017. Acesso em: 12/11/2013

HORITA, Fernando Henrique da Silva; MORAIS, Fausto Santos; OLIVEIRA, Camila Martins. II Congresso Internacional De Direito E Inteligência Artificial: Direito Penal E Cibercrimes. Belo Horizonte: Skema Business School, 2021. Disponível em: http://site.conpedi.org.br/publicacoes/b3vv7r7g/760jvn58/pWhW56Ck65jkj37J.pdf. https://www.buscadordizerodireito.com.br/jurisprudencia/detalhes/fa587ec2731aab9f2952622e89088d4b?palavra-chave=Crimes+Inform%C3%A1ticos&criterio-pesquisa=e&forma-exibicao=apenas-com-informativo&ordenacao=data-julgado. Acesso em: 10/11/2023

JESUS, Damásio; MILAGRE, José Antônio. Manual de crimes informáticos – São Paulo: Saraiva, 2016.

JESUS, Damásio; MILAGRE, José Antônio. Manual de crimes informáticos – São Paulo: Saraiva, 2016.
https://www.buscadordizerodireito.com.br/jurisprudencia/detalhes/fd4d801731725513a4d77aa9bb35534b?palavra-chave=Falsidade+inform%C3%A1tica&criterio-pesquisa=e

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

JESUS, Damásio; MILAGRE, José Antônio. Manual de crimes informáticos – São Paulo: Saraiva, 2016.

JESUS, Damásio; MILAGRE, José Antônio. Manual de crimes informáticos – São Paulo: Saraiva, 2016.

LEITE, George Salomão; LEMOS, Ronaldo Lemos. Marco civil da internet. São Paulo: Atlas 2014.

LEITE, George Salomão; LEMOS, Ronaldo Lemos. Marco civil da internet. São Paulo: Atlas 2014.

LIMA, Paulo Ferreira. Crimes de computador e segurança computacional, Campinas: Millennum, 2006.

https://memoria.ebc.com.br/agenciabrasil/noticia/2004-09-13/pesquisas-apontam-que-brasil-esta-na-rota-dos-crimes-na-internet

MUGGAH, Robert. O problema do cibercrime no Brasil. disponível em: https://brasil.elpais.com/brasil/2015/10/23/opinion/1445558339_082466.html. Acesso em 05/11/2023.

MANZUR, Claudio Líbano. Los Delitos de Hacking en Sus Diversas Manifestaciones. Disponível em: https://vlex.es/vid/delitos-hacking-diversas-manifestaciones-107511

MAGALHÃES, José Luiz Quadros de. Direito constitucional: curso de direitos fundamentais. 3. ed. São Paulo: Método, 2008.

PINHEIRO, Reginaldo César. Os crimes virtuais na esfera jurídica brasileira. Boletim IBCCcrim, ano 8, n. 101. Abr.2001.

SPINIELI, André Luiz Pereira. Crimes cibernéticos: coletânea de artigos. ed 3. Brasilia: MPF, 2018.

https://super.abril.com.br/tecnologia/tem-boi-na-linha-hackers-os-espioes-ciberneticos/

TAVARES, Adriano Lopes; REIS, Rafael Rocha. Crimes de informática. Revista jurídica, n. 23, jan. 2014. Disponível em: revistas2.unievangelica.edu.br/index.php/revistajuridica/article/view/1070/1012 acesso em 30/10/2023

TÔRRES, Fernanda Carolina. O direito fundamental à liberdade de expressão e sua extensão. Disponível em: https://www12.senado.leg.br/ril/edicoes/50/200/ril_v50_n200_p61.pdf

VALENTE, Jonas. Entenda o que é a neutralidade da rede e como é o seu funcionamento no Brasil. disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2017-12/entenda-o-que-e-neutralidade-de-rede-e-como-e-o-seu-funcionamento-no-brasil. acesso em: 04/11/2023