PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS

Programa de Graduação em Direito

Carlos Eduardo Gontijo Costa

CIBERCRIMINALIDADE:
Os crimes cibernéticos e os limites da punibilidade no ambiente virtual

Arcos
2023

Carlos Eduardo Gontijo Costa

CIBERCRIMINALIDADE:

Os crimes cibernéticos e os limites da punibilidade no ambiente virtual

Monografia apresentada ao Curso de Direito da Pontifícia Universidade Católica Minas Gerais,como requisito parcial para obtenção do título de Bacharel em Direito.

Orientador: Profa Maria do Carmo Bernardes Oliveira Metzker

Área de concentração: Direito Processual Penal

Arcos
2023

CIBERCRIMINALIDADE:

Os crimes cibernéticos e os limites da punibilidade no ambiente virtual

Monografia apresentada ao Curso de Direito da Pontifícia Universidade Católica Minas Gerais,como requisito parcial para obtenção do título de Bacharel em Direito.

Área de concentração: Direito Processual Penal

Profa. Maria do Carmo Bernardes Oliveira Metzker

(Banca Examinadora)

(Banca Examinadora)

Arcos, junho de 2023.

AGRADECIMENTOS

A todos os que me ajudaram ao longo desta caminhada. Principalmente à meus pais e familiares;

A minha orientadora, sem o qual não teria conseguido concluir esta importante tarefa..

RESUMO

Esta monografia aborda a aplicação do Código Penal Brasileiro em crimes virtuais e, neste contexto, tenta responder às questões de validação, aplicação e suas possíveis soluções em crimes virtuais. Para abordar esta questão da forma mais abrangente possível, algumas questões extremamente relevantes devem ser abordadas, como o que é é/ou pode ser considerado crime virtual, qual a definição e regulamentação do espaço virtual e suas características, a definição de levantamento localização e jurisdição.O foco principal do estudo é mostrar como as medidas atualmente em vigor, se aplicadas melhor ou corretamente de forma diferente das atuais medidas contidas no código penal brasileiro, seriam mais eficazes na punição. Para saber como esta questão é tratada atualmente, suas implicações, fatos e problemas, dinâmica atual; assim, reunindo suas aplicabilidades e contrastando-as com o ordenamento jurídico brasileiro, e obtendo uma opinião sobre suas respectivas eficiências.

Palavras chave: Crimes. Virtuais. Espaço. Virtual. Punibilidade.

ABSTRACT

This monograph addresses the application of the Brazilian Penal Code in virtual crimes and, in this context, tries to answer the questions of validation, application and its possible solutions in virtual crimes. In order to address this issue in the most comprehensive way possible, some extremely relevant issues must be addressed, such as what is and/or can be considered a virtual crime, what is the definition and regulation of the virtual space and its characteristics, the definition of survey, location and jurisdiction .The main focus of the study is to show how the measures currently in force, if applied better or correctly differently from the current measures contained in the Brazilian penal code, would be more effective in punishment. To know how this issue is currently treated, its implications, facts and problems, current dynamics; thus, gathering their applicability and contrasting them with the Brazilian legal system, and obtaining an opinion on their respective efficiencies.

Keywords: Constitutionality. Evidences. Craft. Systems. Warranties.

SUMÁRIO

1 INTRODUÇÃO

Este trabalho tem por objeto a explanação sobre o surgimento de novos delitos em decorrência do uso da internet, e a necessidade do Direito em acompanhar as mudanças trazidas pela evolução tecnológica.

Nesta baila, os crimes digitais serão tratados nesse contexto de influência da informática no Direito Penal e da necessidade de adaptação do direito à nova realidade tecnológica da sociedade atual. A promulgação da lei 12.737/12 foi o primeiro passo dado no combate a esses crimes. Contudo, além da simples tipificação dos novos delitos decorrentes da influência da evolução tecnológica na sociedade atual, outras questões, diretamente afetadas pelas particularidades características dos crimes cibernéticos, merecem especial discussão.

A sociedade contemporânea, interligada e global, passa cada vez mais rápido por grandes transformações tecnológicas. Em decorrência desse crescimento desenfreado da tecnologia da informação, houve o surgimento de diversas ferramentas para otimizar nosso tempo, ideias e conectar as pessoas a todo tempo. A mais dinâmica e importante delas, a internet, rede mundial de computadores, é capaz de interligar usuários do mundo inteiro, inovação essa que tornou real uma maior facilidade de conexão.

As vantagens e benefícios oferecidos pela internet resultaram na formação da chamada sociedade da informação, caracterizada pela importância cada vez maior da informação e pela dependência vertiginosa dos recursos tecnológicos em atividades do cotidiano. No entanto, a internet, que a princípio surgiu como uma nova tecnologia de comunicação e deveria ser utilizada em prol da sociedade, transformou-se em um instrumento utilizado para a prática de condutas ilícitas demasiadamente perigosas, fruto da fácil adaptação das pessoas às inovações tecnológicas.

A magnificência da tecnologia, velocidade de acesso e a disseminação da informação acrescentaram algumas peculiaridades no tratamento dos crimes cibernéticos. Estes tipos de crimes são caracterizados pela velocidade com que são cometidos e a novidade de sua apresentação ao mundo jurídico, que quando considerados juntamente com a ofensa a um bem jurídico especial, exigem conhecimentos específicos para que se possa chegar aos indícios de autoria e materialidade da infração penal.

Portanto, a discussão desta monografia acerca dos crimes cibernéticos se

mostra muito útil, tendo em vista que, com a evolução tecnológica, a internet se mostrou o principal meio de comunicação e tráfego de informações, transformando o cotidiano da sociedade atual. Todavia, em razão disto se destaca a principal problemática desta monografia: A legislação interna possui eficácia frente ao combate do crime cibernético?

Portanto, a forma e o ponto de desenvolvimento em que estão as legislações internacionais em matéria penal cibernética. A velocidade e novidade com que esses crimes se perpetuam, bem como os bens jurídicos atingidos por esses delitos são peculiaridades que dificultam a investigação criminal e a produção de provas e portanto a necessidade de peritos especializados, a dificuldade na identificação da autoria e a necessidade da produção antecipada de provas.

O aludido tema foi escolhido em virtude de sua contemporaneidade e, mais do que isso, da importância de despertar para um perigoso cenário de violação de direitos subjetivos e objetivos em um ambiente em que a impunidade parece reinar. Isso denota não apenas a relevância jurídica do tema, mas também a sua relevância político-social. Apesar de serem pouco difundidos e haver até certa escassez teórica sobre o tema, é certo que todos os dias milhares de pessoas em todo o mundo são vítimas de crimes cibernéticos de todas as espécies e tipos penais, chegando até mesmo a ultrapassar o número de crimes praticados no mundo real.

Neste viés, ressalta-se que esta monografia é de natureza qualitativa, buscando compreender os ideais acima revelados por meio de perspectivas históricas, culturais, jurídicas e sociais, e construí-la por meio de um arcabouço doutrinário.

Por fim, esta monografia é composta por três capítulos principais: O primeiro capítulo discute o ciberespaço, o conceito de mundo virtual e a virtualização do espaço comunitário.

. O segundo capítulo trata da punibilidade cibernética, algumas noções gerais sobre a cibercriminalidade analisando também as modalidades mais comuns de crimes informáticos.

Por fim, o último capítulo dispõe acerca da regulamentação dos crimes virtuais e sua eficácia no ordenamento pátrio, a lei de crimes cibernéticos e o projeto de Lei 8.045/2010.

2 O CIBERESPAÇO

Quando se fala de espaço, pode-se interpretar como barreiras físicas que impõem limitações ao comportamento e às atividades dos seres humanos, sejam limitações de origem natural ou limitações que os próprios humanos constroem para melhorar ou mesmo dificultar seu modo de vida.

Ao longo da história da humanidade, tais limitações muitas vezes foram as motivações para a conquista de territórios, e a proteção desses territórios influenciou diretamente nossa evolução como sociedade. O conceito de Estado permeia justamente o território físico sobre o qual a população estabelece, possui e exerce soberania sobre esse território (MARTINS, 2012).

No entanto, ainda de acordo com Martins (2012), os espaços virtuais, formados pelas inovações tecnológicas e melhorias nas redes mundiais de comunicação, trazem novas perspectivas para a compreensão das relações interpessoais e até mesmo internacionais pela ausência de barreiras físicas.

Segundo Seabra (2012), a visão tradicional de limites se baseia nas características dos limites políticos, naturais e artificiais, que geralmente se referem aos espaços físicos ou naturais nos quais os humanos vêm atuando ao longo de sua história, com base em fatores políticos, culturais e de segurança.

Assim, por exemplo, o delineamento de limites, como os altos muros de vilas e cidades nos tempos feudais, indicava a necessidade dos humanos obterem segurança e controle sobre locais específicos. Nessa época, além das muralhas externas, havia o isolamento associado aos castelos dos senhores feudais, que eram protegidos por grossas muralhas (LOPES; NETO, 2015).

Por sua vez, os ambientes digitais, virtuais e intangíveis que são utilizados devido ao uso de tecnologias eletrônicas são caracterizados por fronteiras que fogem dessa visão convencional. Seus limites são materialmente invisíveis, dentro dos quais o fluxo e a interação de informações e dados ocorrem intensamente.

.

2.1 Conceito de mundo virtual

O mundo virtual passou a ser conhecido como ciberespaço e pode ser definido como [...] “o domínio das redes de computadores (e dos usuários por trás delas) no qual as informações são armazenadas, compartilhadas e comunicadas online” (SINGER; FRIEDMAN, 2013, p. 13).

Esta natureza transfronteiriça leva a novas perspectivas sobre as noções tradicionais de poder, território e soberania

De acordo com a conceituação de Weber, um Estado é "uma comunidade humana que pretende monopolizar com sucesso o uso legal da força dentro de um território definido" (Weber, 1982, p. 98).

Desta forma, a delimitação das fronteiras é consistente com os poderes que determinados países exercem sobre os territórios. No entanto, o ciberespaço se configura como um ambiente com fronteiras invisíveis, cuja demarcação pode ser vista como um desafio para os governos.

Neste aspecto, o ciberespaço caracteriza-se por influenciar o comportamento humano de múltiplas formas, estimulando mudanças na cultura e no comportamento social ao permitir fluxos de informação em alta velocidade, sendo de natureza transnacional e não possuindo autoridade reguladora central (MARTINS, 2012).

Pressupõe-se, assim, que, assim como os aparatos tecnológicos mudam a forma como vivemos em sociedade, eles também afetam as interações entre os atores nas relações internacionais.

Ou seja, o espaço cibernético não pode ser considerado totalmente virtual e imaterial, pois sua existência está atrelada às raízes de servidores localizados em território físico, de forma que o controle desses servidores por um determinado Estado é visto como questão de soberania nacional.

2.2 Virtualização do espaço comunitário

A legitimação do exercício do poder pelo Estado ocorre por meio da dominação territorial e do reconhecimento de sua soberania estatal. Como resultado, o ciberespaço tem sido visto pela política internacional como a quinta esfera de poder, além de outras esferas tradicionais: terra, água, ar e espaço.

No entanto, não há governança do ciberespaço e, portanto, é responsabilidade do governo promulgar leis nacionais sobre segurança cibernética, comportando-se da maneira como eles vêem o ciberespaço, pois não há regulamentos que possam orientar e/ou limitar o comportamento do Estado nesse espaço (ELSTRUP, 2018).

Dessa forma, “o ciberespaço tem a capacidade de desafiar a soberania estatal, pois pode colocar em xeque a capacidade dos estados de regular o fluxo e o fluxo de informações dentro de suas fronteiras” (KHANNA, 2018, p. 140).

Esses fluxos de informações e dados virtuais atravessam fronteiras terrestres em milissegundos, dificultando muito a filtragem de seu conteúdo, o que pode ser visto como um aspecto que pode desestruturar os sistemas políticos (MARTINS, 2012).

Portanto, de acordo com Nye (2010), alcançar o controle estatal do domínio cibernético sobre os domínios tradicionais é improvável porque o ciberespaço se configura como um domínio de difusão de poder onde, além de controlar o fluxo de informações, é difícil, Barreiras à entrada no mundo online são baixos, permitindo que indivíduos, pequenos estados e atores não estatais participem ativamente.

O uso excessivo da internet pela humanidade é um reflexo disso, demonstrando a dependência digital que se acumulou nos últimos anos. A forma como as pessoas produzem, consomem, comercializam, comunicam, interagem e se comportam política e profissionalmente em suas vidas privadas é influenciada por essas tecnologias e infraestruturas (HERCHEUI et al., 2012).

À medida que as pessoas participam mais ativamente na obtenção do poder de fornecimento de informações, os governos tendem a modificar o uso da tecnologia da informação para manter o controle do domínio cibernético.

Com base nisto,Nye (2010) analisou que os governos de vários países têm se preocupado com a disseminação e controle das informações, e a mídia tem sido perseguida durante as ditaduras justamente por ameaçar a manutenção do poder, mesmo que indiretamente. Além disso, os novos tipos de ataques e agressões que podem ser realizados entre os atores devido ao mundo cibernético mostram que, apesar das vantagens, a dependência digital também traz vulnerabilidades.

Atualmente, o funcionamento de diversos setores considerados essenciais para a sociedade moderna está diretamente relacionado ao setor da Cibernética, e, portanto, o ambiente digital tornou-se o principal meio de relações financeiras, sociais, acadêmicas e funções dos sistemas de comunicação, transporte, energia, etc. (HERCHEUI, 2012).

Sendo assim, a infraestrutura responsável pelo funcionamento desses setores vitais e pode ser definida como “[...] recursos vitais ou centros de gravidade, cuja perturbação pode ter um impacto significativo na segurança nacional e no normal funcionamento da capacidade do país” (SALTZMAN, 2013, p. 43).

Desta forma, as políticas de cibersegurança proliferam em todo o mundo e ganham notoriedade porque a sua aplicabilidade é cada vez mais importante para a manutenção da harmonia social.

3 PUNIBILIDADE CIBERNÉTICA

Os crimes cibernéticos consistem no cometimento de atividades ilícitas por meio do computador ou rede de internet e classificam-se de acordo com a sua forma de cometimento (WENDT; JORGE, 2012).

Diante a ausência de uma legislação específica que abordasse a temática, cabe ao ordenamento penal vigente julgar aquele que comete crime cibernético. De acordo com uma pesquisa desenvolvida pelo site Safernet, entre os principais crimes cibernéticos, estão: pirataria, pornografia infantil, calunia difamação, injúria, estelionato, entre outros (SANTOS; MARTINS; TYBUCSH, 2017).

Com base nisto será posteriormente exposto algumas noções sobre cibercriminalidade e sua classificação em crimes próprios ou impróprios, como também será relatado ao final as espécies de crimes cibernéticos cometidos com maior frequência.

3.1 Noções gerais sobre a cibercriminalidade

No início do milênio, o mundo digital, embora extremamente fascinante, era ainda enigmático e obscuro para o homem comum. Com a popularização e amplo uso da internet nas mais variadas atividades ressurgiram também aquela familiar e genuína preocupação em relação à segurança das informações que eram compartilhadas online, não somente para os governos, mas a todos que faziam uso dela.

Embora o conceito seja antigo, o termo “cibercrime” surgiu somente no final da década de 90, em uma reunião do G-8 que se destinava à discussão do combate a práticas ilícitas na internet de forma punitiva e preventiva. Desde então, o termo passou a ser usado para designar infrações penais praticadas online (D’URSO, 2017).

Entretanto, a progressiva mutação tecnológica dificulta o combate a esses crimes, que estão em constante alinhamento com as novas tecnologias. Assim, com o uso incontido e indiscriminado da internet, alguns indivíduos com conhecimento em informática passaram a se aprimorar e utilizar esses conhecimentos roubar informações criptografadas, como já havia sendo feito há muito tempo, para obter proveito econômico ou ainda, por mera diversão (JESUS; MILAGRE, 2016).

Esses indivíduos ganharam a denominação de hackers, um designativo da era moderna para indivíduos que sempre existiram. O termo importado da língua inglesa é usado para designar programadores muito habilidosos, alguém que secretamente

alcança informações sobre o sistema informático de outra pessoa para que possam olhar, usar ou trocá-lo , pelos mais variados motivos.

Desta forma, com o desenvolvimento e popularização da internet, a quebra de códigos e invasão de sistemas deixou de ser um instrumento de guerras para se tornar uma oportunidade de lucro ilícito ou mero passatempo, fazendo do cibercrime a mazela social que é hoje (TOLEDO, 2017).

Os estelionatários, por exemplo, viram nas transações comerciais via internet uma oportunidade de aplicar seus golpes. Atraídas pela facilidade de comprar e receber produtos sem sair de casa ou transacionar com suas contas bancárias através de uma tela de computador, as pessoas abraçaram esse novo mercado, sem muita preocupação em apurar a autenticidade dos sites em que estavam inserindo suas informações, o que as fizeram presas fáceis desses criminosos, que agem no submundo da internet.

Todo o tipo de conduta delituosa é praticada online, desde pedofilia, prostituição, tráfico, pirataria, até sabotagem e terrorismo. A digitalização dos métodos de trabalho tem causado em muitos países, inclusive no Brasil, transtornos provocados por uma nova onda de crimes cibernéticos. Só neste ano foram registrados inúmeros sequestro de informações de empresas e hospitais por todo mundo (TOLEDO, 2017).

Embora as formas de praticar crimes na internet estejam evoluindo, o Brasil já possui um longo histórico de condutas informáticas danosas. Outro exemplo dessa infeliz estatística é o do ex-prefeito Paulo Maluf, o qual, nas eleições de 2003, foi o primeiro político a sofrer sabotagem digital. Os hackers invadiram o site do político e espalharam e-mails a todos os eleitores cadastrados, divulgando mensagens de cunho difamatório (TOLEDO, 2017).

Todavia, o direito brasileiro vem lidando com essa questão dos crimes virtuais há muito tempo, e lentamente tem alcançado os infratores da norma no plano virtual e aplicado punições no mundo real. Além das alterações no Código Penal Brasileiro, que inseriu infrações cibernéticas no bojo da lei através da Lei 12.737/2012, apelidada de “Lei Carolina Dieckmann”, temos ainda o ECA (Lei 8.069/90), a Lei de Software (Lei antipirataria nº 9.609/98), a Lei de Racismo (Lei nº 7.716/89) e a Lei de Segurança Nacional (Lei 7.170/83), compondo o conjunto de normas mais relevantes aplicáveis ao cibercrime. Sob outro aspecto, existem crimes praticados contra os direitos básicos do cidadão, garantidos pela Constituição Federal, como a igualdade, a privacidade e a intimidade têm sido sobrepujadas e violadas (ANDREUCCI, 2017).

Além da Lei 12.737/2012, a legislação brasileira conta ainda com o Marco Civil da Internet, Lei 12.965, em vigor desde 2014, compondo o conjunto de normas cibernéticas, o qual prevê princípios, garantias, direitos e deveres para o uso da internet

no Brasil e ainda determina as diretrizes para atuação dos entes federativos em relação à matéria. Embora a Lei do Marco Civil estabeleça sanções para a inobservância de algumas de suas normas, não prevê qualquer tipo de infrações cibernéticas propriamente ditas (ANDREUCCI, 2017).

Existem ainda leis que regulam o uso da internet, mas nenhuma que preveja nem puna os tipos de infrações mais graves praticadas online, especificamente. A maneira de legislar do judiciário brasileiro é temerária e, por vezes, incompreensível, pois estabelece padrão de conduta relacionado à sociedade, ao invés de prever e determinar punições a condutas erráticas, especialmente quando se fala de delitos de alto nível como o roubo ou o sequestro de informações.

Outra norma que prevê delitos cibernéticos é a Lei de Segurança Nacional (Lei nº 7.170/83), porém, relacionam-se apenas aos crimes contra a segurança nacional, a ordem política e social, não prevendo quaisquer das outras condutas mais comumente praticadas através da internet. A Lei de Software, por outro lado, que dispõe sobre a propriedade intelectual de programas de computador, também não prevê a prática de condutas delituosas online (ANDREUCCI, 2017).

Por fim, temos o Estatuto da Criança e do Adolescente, que é o que melhor se destaca entre os demais, pois a lei não apenas dispõe de rol de crimes em espécies, praticados contra a segurança, bem-estar e integridade física e moral da criança e do adolescente, também através da internet, como ainda dispõe acerca dos procedimentos investigativos a serem realizados por agentes da polícia na internet.

Portanto, a internet se tornou um meio de comunicação e debate muito eficaz que, embora útil, tem sido usada levianamente, especialmente por crianças e adolescentes. Eis a importância do ECA frente a esse novo meio de interação social.

3.2 Análise das modalidades mais comuns de crimes informáticos

A partir do momento que a criminologia percebeu que a internet se tornou um novo foco de criminalidade, foi necessária a criação de teorias para definir os crimes virtuais, bem como entender por qual razão eles ocorrem (JAISHANKAR, 2007).

No Brasil, a infração penal é o gênero, podendo ser dividida, estruturalmente, em crime (ou delito) e contravenção penal. As condutas mais graves, por consequência, são etiquetadas pelo legislador como crimes, enquanto as menos lesivas, como contravenções penais (CUNHA, 2014).

Não cabe, no presente trabalho, trazer as distinções entre crime e contravenção penal, sendo apenas importante determinar que quando se utiliza a expressão “crimes virtuais” fala-se no mesmo sentido de infração penal (gênero).

O que realmente importa para a análise são as suas características. Guilherme de Souza Nucci conceitua crime da seguinte maneira:

> Poucos institutos sobreviveram por tanto tempo e se desenvolveram sob formas tão diversas quanto o contrato, que se adaptou a sociedades com estruturas e escala de valores tão distintas quanto às que existiam na Antiguidade, na Idade Média, no mundo capitalista e no próprio regime comunista (NUCCI, 2011, p. 173).

Já os crimes virtuais, além das características das infrações penais “reais” são identificados como cometidos através do uso de dispositivos tecnológicos. Alguns doutrinadores como o Professor Marcelo Xavier de Freitas Crespo (2011) se utilizam de outras nomenclaturas para tratar dos crimes virtuais.

Em que pese não existir consenso entre os doutrinadores que abordam o tema e a diversidade de nomenclaturas acerca do tema, todas abarcando as diversas condutas ilícitas realizadas por algum tipo de dispositivo tecnológico, a que ser utilizado neste trabalho a de “Crimes Virtuais” por entender-se que a realização das condutas é dada em um ambiente virtual (SYDOW, 2014).

Corroboram com esse conceito os professores Damásio de Jesus e José Antônio Milagres (2016), quando arrematam que crimes virtuais são fatos típicos e antijurídicos cometidos por meio da ou contra a tecnologia da informação, ou seja, um ato típico e antijurídico, cometido através da informática em geral, ou contra um sistema, dispositivo informático ou redes de computadores.

Importante lembrar-nos que a função do Direito Penal consiste em coibir condutas divergentes daquelas tipificadas, impondo sanção e protegendo bens jurídicos. Para isso, uma estrutura normativa é gerada, criando uma lógica própria.

Com base nisto, traz-se a ideia de uma classificação mais precisa de delito informático, dividindo o delito em quatro tipos, crimes de informática próprios e crimes de informática impróprios, como expresso abaixo.

3.2.1 Crimes informáticos próprios

Os Crimes Cibernéticos próprios, ou também conhecidos como puros são aqueles em que o agente necessita imprescindivelmente do computador para realizar ataques remota ou diretamente com uso de sistemas informáticos todo o bem jurídico já

tutelado. Nesta situação estão envolvidas não só a invasão e captura dos dados salvos em massa, mas também a intenção de alterar, inserir, adulterar ou destruir dados existentes no computador (SYDOW, 2014).

Nesta linha de pensamento, Viana, (2003, p. 13-26), diz que: “São aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados).”

Ainda nesse contexto, Jesus se posicionam da seguinte forma:

> Crimes eletrônicos puros ou próprios são aqueles que sejam praticados por computador e se realizem ou se consumem também em meio eletrônico. Neles, a informática (segurança dos sistemas, titularidade das informações e integridade dos dados, da máquina e periféricos) é o objeto jurídico tutelado (JESUS, 2016, p,245).

Destacamos também a presença de duas figuras nesta mesma conjuntura: os hackers e os crackers. Segundo a pesquisa ao dicionário Michaelis, um dos significados do termo hacker é: “pessoa que usa seu conhecimento técnico para ganhar acesso a sistemas privados” (SYDOW, 2014, s.p).

Fazendo uma análise sobre a acepção desta palavra, podemos concluir que esta é a pessoa que detém um conhecimento singular acerca do assunto e que não necessariamente o use com o propósito de atuar na ilegalidade porque a partir desse discernimento conclui-se que o domínio no referido assunto pode ser visto de forma positiva e negativa. Já os crackers são pessoas que agem focando na vantagem ilícita. Eles invadem e destroem sites, sejam eles quais forem, fazem quebra de senhas, desenvolvem softwares capazes destruir várias máquinas ao mesmo tempo.

Ou seja, os crimes informáticos , são aquelas condutas antijurídicas e culpáveis que visam atingir um sistema informático ou seus dados violando sua confiabilidade, sua integridade e/ou sua disponibilidade.

3.2.2 Crimes informáticos impróprios

Os crimes cibernéticos impuros ou impróprios são aqueles que são praticados com o uso do computador. Diferente dos crimes cibernéticos Puros, esta forma de delito usa o computador como um mero instrumento para a realização deste. Entretanto, os crimes que são realizados com este “auxílio" já são tipificados pelo Código Penal Brasileiro demonstrando que o uso do PC não é um fator primordial mas sim uma das diversas formas de materializar uma conduta delituosa que já está tutelada. Desta forma, Jesus demonstra:

> [....] Já os crimes eletrônicos impuros ou impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço "real", ameaçando ou lesando outros bens, não computacionais ou diversos da informática(JESUS, 2013, p.247).

Tendo como base essa distribuição se torna mais acessível e mais compreensível o entendimento sobre o que vem a ser os crimes cibernéticos Puros e os Impuros, enfatizando sempre que um necessariamente precisa do computador, vez que a outra modalidade precisará do PC apenas como instrumento para a realização do delito.

Os crimes virtuais impróprios mais recorrentes do mundo digital são velhos conhecidos dos ordenamentos jurídicos, tais como crimes contra a honra, discriminação, ameaça, fraude, falsidade ideológica entre outros, sendo que, agora, existem mais ocorrências dos mesmos. No caso da internet a possibilidade do anonimato estimula o descumprimento de regras, pois gera maior certeza de impunidade (PINHEIRO, 2014).

Portanto, os crimes impróprios, são condutas comuns – típicas, antijurídicas e culpáveis – que são perpetradas utilizando-se de mecanismos informáticos como ferramenta, mas que poderiam ter sido praticadas por outros meios.

3.3 Os principais ataques cibernéticos de acordo com as agências de segurança

Para a análise desta monografia, buscou-se identificar quais são, atualmente, os principais ataques cibernéticos de acordo com as agências de cibersegurança.

Essa análise é importante porque, segundo pesquisa da empresa de cibersegurança Norton , realizada em maio de 2021, estima-se que mais da metade dos internautas já sofreram algum tipo de ataque, sendo que 35% deles foram vítimas nos 12 meses antecedentes à pesquisa. Dada a característica de transnacionalidade dos atuais delitos cibernéticos, tal análise se faz necessária tanto a nível nacional quanto internacional (THE HARRIS POLL, 2021).

De acordo com a Agência Brasil, em 2020, o país chegou a um total de 152 milhões de pessoas com acesso à internet, o que representa aproximadamente 81% da população com mais de 10 anos (LEON, 2021).

Segundo dados da Fortinet, empresa multinacional do ramo da cibersegurança, foram registrados, entre os períodos de janeiro a junho de 2021, 16,2 bilhões de tentativas de ataques cibernéticos apenas no Brasil (ASSOCIAÇÃO DE EMPRESAS E PROFISSIONAIS DA INFORMAÇÃO, 2021).

Apesar dos números alarmantes, o país ainda não conta com um serviço consolidado de notificação e tratamento desses incidentes, motivo pelo qual os dados encontrados ainda estão muito aquém da realidade. Tentando sanar este problema,

institui-se o CERT.br como receptor de notificações relacionadas a incidentes cibernéticos no país e o CTIR Gov, responsável pelas notificações relacionadas aos órgãos da administração pública.

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) é um Grupo de Resposta a Incidentes de Segurança (CSIRT) de responsabilidade nacional, mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil. Como um de seus serviços, o CERT.br mantém dados estatísticos sobre notificações de acidentes a ele reportados. Ressalte-se que estas notificações são voluntárias e refletem apenas os incidentes ocorridos em redes que espontaneamente notificaram ao órgão.

De acordo com o relatório da agência12, no ano de 2020, os ataques do tipo Scan foram os mais reportados, responsáveis por 58,85% das notificações. Em seguida, encontram-se os ataques do tipo Worm (20,15%), DoS (10,25%), Fraude (4,60%), Web (3,99%) e Invasão (0,18%). Dentre os ataques, 0,97% foram classificados como “Outros” (CERT.br, 2020).

Apesar da aparente imprecisão na adoção do termo “fraude”, verificou-se que o CERT.br utiliza essa tipologia para designar ataques do tipo Engenharia Social - Phishing e ataques do tipo Cavalo de Tróia.

Em relação aos ataques do tipo Web, a agência os define como um caso particular de ataque visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet. Por se tratar de um termo bastante genérico e que engloba uma variedade de ataques, como DDoS e Ransomware, que serão tratados individualmente, restringirmos os ataques Web aos tipos que geram desfigurações de páginas na Internet. Esses ataques, também conhecidos como Defacement, são responsáveis por 61,2% dos ataques Web de acordo com o CTIR Gov (CENTRO DE PREVENÇÃO AO TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS DE GOVERNO, 2021).

Em relação à Administração Pública, o Centro de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos (CTIR Gov) é o órgão do governo responsável por receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança cibernética. O Centro está enquadrado na categoria "CSIRT de responsabilidade nacional de coordenação" e tem por objetivo coordenar e integrar ações destinadas à gestão de incidentes computacionais em órgãos ou entidades da Administração Pública Federal.

Em relação às ameaças a nível mundial, coletou-se dados referentes à União Europeia, aos Estados Unidos da América e à Interpol. Essa análise se faz importante

uma vez que, mesmo que esses crimes não tenham ocorrido contra usuários situados no Brasil, uma parte deles tem sua origem em território nacional. Segundo a empresa de cibersegurança Kaspersky , mesmo que não seja o principal alvo, o Brasil é o líder mundial em botnets multifuncionais, tipo de ataque utilizado para derrubar ou paralisar o serviço de grandes empresas, como Amazon, Netflix e CNN (FUTURE, 2017).

A ENISA é responsável por divulgar, anualmente, o ENISA Threat Landscape (ETL), um relatório sobre o estado do cenário de ameaças à segurança cibernética que identifica as principais ameaças, principais tendências observadas em relação a ameaças, seus atores e técnicas de ataque, além de descrever medidas relevantes de mitigação (EUROPEAN UNION AGENCY FOR CIBERSECURITY, 2021).

Em análise à nona edição, referente ao período entre abril de 2020 e julho de 2021, a agência classificou os seguintes ataques como principais ameaças: Ransomware, também classificado como sendo a principal; "*malware"*; "*cryptojacking"*; ameaças relacionadas à e-mail; ameaças contra dados; ameaças contra disponibilidade e integridade; desinformação/informações erradas e ameaças não maliciosas (ENISA, 202).

Finalmente, como última agência pesquisada, selecionou-se dados provenientes da Interpol. A Interpol, ou Organização Internacional de Polícia Criminal, é uma organização intergovernamental que serve para conectar agências policiais de 195 países, facilitando o compartilhamento e acesso a dados sobre crimes e criminosos.

A Interpol é mais uma ferramenta utilizada em prol da Cooperação Internacional em matéria criminal. O relatório da Interpol (2020) trata especificamente dos crimes cibernéticos que aumentaram com o avanço da pandemia de COVID-19.

De acordo com a organização, devido à súbita necessidade de implementação de estruturas de teletrabalho, empresas em todo o 38 mundo precisaram desenvolver rapidamente sistemas, redes e aplicações remotas. Como resultado, "[...] criminosos estão tirando vantagem das crescentes vulnerabilidades de segurança decorrentes do trabalho remoto para roubar dados, gerar lucros e causar danos" (INTERPOL, 2020, p.4).

Segundo os dados do relatório, os ataques do tipo Phishing, Scam e Fraudes foram os delitos que mais apresentaram alta, sofrendo um aumento de 59%. Em segundo lugar aparecem os ataques do tipo Malware/Ransomware, com alta de 36%. Os ataques do tipo Domínios Maliciosos sofreram um aumento de 22%, seguidos das ameaças do tipo Fake News, que aumentaram 14% (INTERPOL, 2020).

Ressalta-se que para a realização do estudo, a INTERPOL contou com dados de 194 países, além de informações fornecidas pelo setor privado e pelo Grupo de Trabalho Regional em Cibercrime da própria organização.

4 A REGULAMENTAÇÃO DOS CRIMES VIRTUAIS E SUA EFICÁCIA NO ORDENAMENTO PÁTRIO

4.1 A lei de crimes cibernéticos

São princípios constitucionais, previstos no art. 5. XXXIX da Constituição Federal de 1988, Princípios da reserva legal e da legalidade. Portanto, não podem ser considerados crimes os atos não regulamentados pela lei e os atos praticados sem tramitação legal.

Para Silva, o princípio da legalidade, ou preservação legal, caracteriza-se por uma limitação dos poderes punitivos do estado, bem como uma limitação dos poderes normativos do estado, porque impede a criação de tipos penais, fora do processo legislativo normal.

Segundo os autores, este princípio é “resultado direto dos fundamentos da [….] dignidade humana, pois remonta à ideia de preservação e desenvolvimento de quem a possui” (SILVA, 2011, p.7)

O Código Penal brasileiro confirma essa previsão em seu artigo 1º, afirmando que "Não há crime sem prévia definição legal". Não há pena sem prévia sanção legal" (BRASIL, 1940).

Considerando a obrigatoriedade de previsão legal que pune os atos proibidos, no que se refere aos crimes virtuais, até 2012 não havia legislação para punir os crimes virtuais propriamente ditos, ou seja, crimes contra dispositivos e sistemas de informação.

A legislação penal vigente permite a punição de crimes virtuais impróprios, pois incluem crimes já típicos do ordenamento jurídico brasileiro, com a especificidade da utilização de computadores como meio criminoso.

Há algum tempo, diante do desenvolvimento da tecnologia e da falta de normas punitivas específicas para proteger os usuários, vítimas de crimes digitais, vários projetos de lei visando regulamentar tais crimes tramitam no Congresso, entre eles a Lei nº 2.126/11, que institui um Código Civil de Marcas ; Projeto de Lei 2.793/11, do Deputado Paulo Teixeira; e Projeto de Lei 84/99, do Deputado Eduardo Azeredo (PINHEIRO, 2013).

Como resultado de incidentes, incluindo vários ataques de negação de serviço em sites do governo brasileiro em meados de 2011, os sites ficaram instáveis até ficarem offline, resultando, conforme revelado anteriormente, no ataque contra a atriz Carolina Dickman, onde 36 fotos da atriz foram roubadas de seu site por hackers em 30

de novembro de 2012, sendo postadas na Internet, o que ajudou a aprovar leis específicas sobre o assunto em caráter de urgência para preencher a lacuna do ordenamento jurídico.

No que diz respeito às lacunas existentes nos crimes digitais, a Lei n. foi aprovada e promulgada a Lei nº 12.735, que dispõe sobre a necessidade de criação de órgão especializado em investigação, e a Lei nº 12.737, que incorpora o tipo penal de invasão de equipamento de informática ao Código Penal Brasileiro (art. procedimento desse crime (art. 154-B), retirado do Código Penal Brasileiro (PINHEIRO, 2013).

Além de incluir esses dois meios, a lei também alterou a redação de dois delitos existentes previstos no art. Seção 266 do Código Penal, Interrupção ou Interrupção de Telégrafo, Telefone, Computador, Telemática ou Serviços de Informação de Utilidades; e o artigo 298.º do Código Penal para a falsificação de documentos particulares que passou a equiparar os cartões de crédito e de débito aos documentos particulares referidos no artigo.

Portanto, atos de uso não autorizado de dados de cartões de crédito e débito obtidos indevidamente, invasão de dispositivos eletrônicos conectados ou não à Internet, produção, fornecimento e venda de programas de computador que permitam a infecção de vírus da Internet e acesso a informações confidenciais ou violação de privacidade Comunicação eletrônica ou segredo comercial.

Em breve análise das novas infrações penais criadas com o advento da Lei 12.737, Patrícia Peck Pinheiro afirma:

> Ainda, receberá as mesmas penas da invasão aquele que instala uma vulnerabilidade em um sistema de informação para obter vantagem indevida, por exemplo, um backdoor ou uma configuração para que algumas portas de comunicação à internet fiquem sempre abertas. O usuário de gadgets e dispositivos informáticos comuns estão protegidos contra hackers e pessoas mal intencionadas que abusam de confiança ou buscam intencionalmente devassar dispositivo para se apropriar de dados do computador ou prejudicar o seu proprietário, com a exclusão ou alteração de dados, para que fiquem imprestáveis, ou ainda, informações íntimas e privadas, como fotos, documentos e vídeos. As empresas possuem maior proteção jurídica contra a espionagem digital, pois a obtenção de segredos comerciais e ou informações sigilosas definidas por lei agora também se enquadram na lei (PINHEIRO, 2013, 308).

Dois dispositivos legais foram aprovados, traduzidos em common law e publicados no Diário Oficial da União em 3 de dezembro, demonstrando a preocupação com a vulnerabilidade de quem acessa a internet e busca a proteção do Estado. No entanto, embora a ratificação dessas leis represente o primeiro passo para a discussão de tais crimes no âmbito do direito digital, punindo condutas até então não tipificadas, ainda há muito o que se discutir quando se trata de crimes cibernéticos.

Para combater o cibercrime, há questões que precisam ser discutidas além das questões conceituais relacionadas à classificação dos crimes. Outras inovações legais, como a produção de provas (investigação de provas) em crimes digitais, devem ser discutidas a fim de criar uma base legal suficiente para fortalecer o direito penal diante de novas infrações penais.

4.2 A legislação interna possui eficácia frente ao combate do crime cibernético? A dificuldade para produção de provas

Os avanços tecnológicos e as novas descobertas científicas levaram ao surgimento de uma nova realidade para a humanidade. O espaço cibernético, um novo ambiente social em que a prática dos comportamentos e dos fatos jurídicos existe independentemente do espaço e da presença física, é o motor que permite a emergência dessa nova realidade (MALAQUIAS, 2012, p. 59).

O desenvolvimento da tecnologia, além de permitir o manuseio e processamento automatizado de informações e telecomunicações em diversas esferas da vida, também tornou a prática do crime informático mais diversificada e perigosa. Nas palavras de Crespo: “A evolução tecnológica da sociedade pressupõe a evolução tecnológica dos comportamentos ilícitos, tanto ao nível dos meios como dos objetos” (CRESPO, 2011, p. 115).

O cibercrime é cada vez mais caracterizado pela variedade e periculosidade que apresenta, criando maiores dificuldades na investigação e comprovação desses crimes, bem como na elaboração de perícias e estabelecimento de autoria, entre outras questões.

Neste capítulo, serão apresentadas as principais questões da monografia, um estudo sobre a eficácia jurídica do combate ao cibercrime e as dificuldades de obtenção de prova no processo penal sob o ponto de vista dos crimes virtuais, um levantamento que identifica os principais aspectos que devem ser repensados no modelo atual do Brasil.

No ordenamento jurídico pátrio, não há barreiras ao uso de provas eletrônicas, como o art. 225 do Código Civil:

> As reproduções fotográficas, cinematográficas, os registros fonográficos e, em geral, quaisquer outras reproduções mecânicas ou eletrônicas de fatos ou de coisas fazem prova plena destes, se a parte, contra quem forem exibidos, não lhes impugnar a exatidão (BRASIL, 1940, s.p).

Também merece destaque a Medida Provisória 2.200-1/2001, que institui a Infraestrutura Brasileira de Chaves Públicas - ICP Brasil, que já em seu art. 1º versa sobre sua finalidade.

Caso o documento eletrônico não esteja assinado, ou caso o certificado não esteja vinculado à ICP-Brasil, pode ser realizada checagem informatizada para verificar a autenticidade do documento, credenciamento como selo de qualidade técnica, e não prevalecerá na avaliação da prova, como o juiz tem condenação por motivo livre, ele avaliará livremente a prova.

As pessoas agora podem usar assinaturas digitais e certificados digitais, que são técnicas de criptografia que usam uma ferramenta de codificação para enviar informações seguras por redes eletrônicas.

Uma assinatura eletrônica é uma chave privada, um código pessoal não reproduzível que impede que o conteúdo transmitido seja lido apenas por destinatários que possuem a mesma chave e são identificados como tendo a mesma validade de uma assinatura tradicional (PINHEIRO, 2010).

Os certificados digitais são uma grande ferramenta no mundo atual, pois conferem autenticidade aos documentos virtuais, não deixando dúvidas quanto à sua origem. Quando um usuário navega na Internet, é atribuído a ele um número IP - o Internet Protocol é esse número que permite que o usuário seja identificado na rede, ou investigue algum crime ocorrido, o problema é que esse número só é atribuído a o usuário no momento da conexão, aqui Após o período, ao desligar o modem, o endereço IP será atribuído a outro usuário caso não tenha selecionado um IP fixo. Quando solicitado pelo provedor de acesso à Internet, o IP deve vir acompanhado da data, hora da conexão e fuso horário do sistema, dados esses imprescindíveis, tendo em vista que sem eles é impossível quebrar o sigilo dos dados.

Uma vez localizado o provedor, o juiz deve exigir que os dados telemáticos sejam mantidos em sigilo para que o provedor de acesso saiba quem estava associado ao endereço IP no momento do crime, ou seja, seu endereço real (PINHEIRO, 2010).

O crescente uso de computadores e da Internet para cometer crimes levou à necessidade de investigar crimes cometidos em redes globais de computadores. Assim surgiu a perícia forense computacional, cujo objetivo é investigar e coletar indícios de atos ilícitos cometidos por meio de computadores (RODRIGUES; FOLTRAN JR, 2010).

Toda investigação começa com as evidências e informações coletadas, e o ambiente virtual é indistinguível do ambiente físico. No caso do cibercrime, as provas podem ser obtidas a partir de qualquer dispositivo eletrônico (telefone celular, disco rígido).

Ou seja, evidência digital pode ser definida como toda informação obtida em formato compreensível por humanos a partir de compilações ou repositórios eletrônicos, com ou sem intervenção humana (PINHEIRO, 2013).

Nas investigações de crimes digitais, devido à volatilidade e falsificação de dados, as provas eletrônicas devem passar por rigorosa perícia técnica antes de serem aceitas no processo para garantir a validade e integridade dos resultados. Esse é o objetivo da computação forense: provar o mais claramente possível o que aconteceu.

A computação forense é uma ciência responsável por elucidar fatos, coletar, verificar e avaliar evidências digitais por meio de métodos científicos, para que os infratores sejam punidos. O objetivo da perícia forense computacional é extrair o máximo de informações ao analisar vestígios relacionados a um crime, levando a conclusões (PINHEIRO, 2013).

Ou seja, a computação forense é uma especialidade caracterizada pelo exame científico e sistemático de computadores, por meio da coleta de evidências digitais, buscando tirar conclusões sobre casos investigativos. Os eventos descobertos são reconstruídos, o que permite determinar se o computador analisado foi usado para realizar atos ilegais ou não autorizados.

Exemplos de evidências que podem ser úteis na investigação de crimes digitais incluem: arquivos gráficos de pornografia infantil, mensagens eletrônicas com ameaças e chantagens, arquivos com informações incriminatórias ou dados roubados (PINHEIRO, 2013).

Por serem desenvolvidos e aperfeiçoados em um ambiente virtual caracterizado pela ausência física do sujeito ativo, os crimes virtuais são muitas vezes considerados crimes bastante complexos, uma vez que o infrator existe inteiramente em um espaço cibernético.

Somando-se a essa complexidade está a facilidade com que as evidências (fotos, vídeos, arquivos digitais, dados) fornecidas para tais crimes podem desaparecer facilmente. Ou seja, como é fácil modificar, perder ou até deletar tais evidências.

Os crimes digitais são difíceis de provar. Por um lado, existe a comodidade de cometer crimes por meio de computadores, por outro lado, a verificação de vestígios exige habilidades técnicas específicas, que não estão disponíveis em todos os locais de crime.

A fragilidade da natureza modificada dos documentos digitais exige a nomeação de peritos tecnicamente qualificados para confirmar a autenticidade dos documentos. Embora a computação forense seja muito precisa, a coleta de evidências torna-se frágil. Se for feito de forma errônea, em desacordo com o disposto na lei substantiva ou nos

princípios constitucionais, pode tornar a prova ilegal ou inválida. A produção de provas ilícitas pode ser extremamente prejudicial ao processo, pois tal prova contamina toda prova dela produzida (TÁVORA, ALENCAR, 2012).

Assim, todas as provas provenientes de provas ilícitas devem ser afastadas do processo nos termos do artigo 157.º do Código de Processo Penal, segundo o qual são inadmissíveis e devem ser afastadas do processo, entendendo-se por provas ilícitas aquelas obtidas com violação das normas constitucionais ou legais.

Devido ao rigor exigido desse tipo de perícia, o maior problema jurídico na obtenção de provas em crimes virtuais é o preparo insuficiente da polícia investigativa e da perícia. Poucos profissionais estão preparados para esse tipo de investigação e, como tal, devem ser altamente qualificados e profissionais para lidar com a perícia focada em investigações de crimes digitais para atender aos requisitos técnicos de coleta e custódia para evitar contestações de identidade e a legalidade da obtenção de provas (TÁVORA, ALENCAR, 2012).

As investigações criminais e a orientação processual requerem procedimentos técnicos a fim de legitimar as provas geradas nos crimes virtuais. Profissionais especializados em hardware, software, tráfego e segurança de redes passarão por perícias para apontar a verdade. A eficácia das investigações criminais dependerá da atuação desses peritos na análise do ambiente criminal e na verificação da autenticidade.

Ao analisar o ambiente em que ocorreu o crime, os profissionais poderão verificar se há vestígios da atividade criminosa. Roberto Antônio Malaquias cita o exemplo de envio de e-mails não autorizados, dando exemplos de rastros que podem indicar violação, como indicação de origem, autor, destinatário, adulteração, rota utilizada para chegar ao destino final do e-mail, endereços virtuais e protocolos de comunicação envolvidos identificarão o caminho percorrido pela mensagem na rede de computadores. Nesse exemplo, a identificação do e-mail, da investigação criminal e do objeto da prova e todos os seus componentes serviriam de rastreador para identificar a máquina de onde tal mensagem foi enviada como prova documental (COLLI, 2010, p. 160).

Diante da necessidade de especialização dos profissionais responsáveis pela investigação de crimes digitais, Maciel Colli disse que a criação de um departamento especializado em informática, mídia e meios de comunicação pode ser uma das formas de solucionar alguns dos problemas relacionados ao cibercrime. Devido à rapidez e novidade com que ocorrem os crimes contra bens jurídicos especiais (informação), gera-se conhecimento específico para que se obtenham provas da autoria e do significado das infrações penais (COLLI, 2010).

No Brasil, sob a jurisdição da polícia civil, sete estados possuem departamentos de polícia dedicados à investigação de crimes cibernéticos. No âmbito da Polícia Federal, o combate aos crimes cibernéticos está atualmente sob a responsabilidade da Unidade de Crimes Cibernéticos (URCC) da Polícia Federal.

Embora o país esteja se preparando para combater o cibercrime com a criação de delegacias especializadas e treinamento de profissionais encarregados de investigar tais crimes, não há profissionais suficientes nesta área para investigar as atividades ilegais que ocorrem todos os dias nas redes globais de computadores. Em uma era de cotidiano que inclui crimes, o papel dos especialistas em computação é extremamente importante, responsáveis por desvendar e solucionar crimes que exigem conhecimentos específicos.

4.3 A produção antecipada de provas como resposta a ineficácia da legislação em produzir provas

Investigações criminais realizadas pela polícia judiciária, cujo objetivo é a recolha de provas de um crime para identificar os factos típicos e os alegados autores, ou seja, o objetivo da investigação é identificar o crime e os seus autores. As investigações se materializam em autos conhecidos como inquéritos policiais.

Quando um crime é cometido, o Estado tem o poder e o dever de punir o suposto autor. A existência de elementos de informação sobre a autoria e o significado da violação é um pré-requisito necessário para que o Estado inicie um processo criminal no tribunal. Ou seja, para se instaurar uma ação penal contra alguém, é necessário um conjunto mínimo de provas que apontem a prática da conduta criminosa e a probabilidade de o acusado ser o autor (LOPES JR, 2012).

O inquérito policial é procedimento administrativo preventivo. Conforme estipulado no art. O n.º III do artigo 6.º do Código de Processo Penal é normalmente uma instrução provisória, uma vez que as autoridades policiais devem “recolher todos os elementos de prova que contribuam para o esclarecimento dos factos e das suas circunstâncias” com vista a instruir futuras condutas criminosas. No entanto, além da coleta de depoimentos, documentos ou provas periciais, as investigações podem resultar em ações intempestivas, como buscas, apreensões e perícias.

O inquérito policial pode, assim, ser definido como um procedimento administrativo investigativo e preparatório correspondente à realização de uma série de diligências tomadas pelas autoridades policiais para colher informações sobre a origem e significado dos fatos. Ou seja, o interrogatório policial criminal corresponde à

investigação e investigação conduzida pela polícia judiciária quando ocorre um crime criminal, tentando apurar quem é o autor do crime.

Tendo em conta o caráter instrumental do inquérito policial, Renato Brasileiro atribuiu ao inquérito policial duas funções, no sentido de esclarecer os crimes cometidos de forma a subsidiar o prosseguimento do processo penal: a função de preservação e a função de preparação. Enquanto a primeira evita a instauração de processo injustificado, a segunda fornece ao titular da ação penal os elementos para que possa iniciá-la, além de resguardar provas que possam se perder no processo (BRASILEIRO, 2014).

O principal objetivo de uma investigação policial é reunir informações sobre os perpetradores e o significado de um crime. No entanto, elementos de informação não devem ser confundidos com evidências.

Um dos princípios norteadores do processo penal é o princípio do contraditório, ou seja, quando uma das partes apresenta provas específicas, a outra parte tem o direito não só de se pronunciar sobre essa prova, mas também de apresentar prova contrária. Segundo Lemos, “toda prova admite contraprova, sendo inadmissível a produção de uma delas sem o conhecimento da outra” (LEMOS, 2010, p. 325).

O contraditório é a condição de existência e validade da prova; sem ele, o nome da prova seria impróprio.

Com as alterações trazidas pela Lei 11.690/2008, o Código de Processo Penal passou a estipular a distinção entre elementos de prova e de informação. Enquanto as evidências admitem contradições e amplas defesas, o elemento de informação exclui tais agências. Ou seja, a prova só pode ser utilizada para se referir aos elementos de convicção produzidos durante o processo judicial, sujeitos ao contraditório e às defesas suficientes; os elementos de informação são colhidos na fase investigativa, não havendo obrigatoriedade de observar o contraditório e as defesas suficientes .

O valor probatório da investigação é considerado relativo, dada a inexistência de provas conflitantes na fase investigativa policial em fornecer informações sobre a autoria e significado do crime. Para Aury Lopes Jr., o inquérito policial tem poder probatório limitado, pois produz apenas comportamento investigativo (LOPES JR, 2012).

Considerando a relativa natureza do valor probatório do inquérito policial por exigir a comprovação de outros elementos colhidos na ordem processual, o Código de Processo Penal dispõe em seu artigo 155 que os magistrados, além da lei, não podem considerar apenas elementos de as informações prestadas como meio de condenação do arguido.

Os magistrados não podem decidir pela condenação do arguido apenas tendo em conta os dados recolhidos durante a fase de inquérito. Nas palavras de Nestor Távora e Rosmar Alencar, “É fundamental que a prova em tribunal seja ditada por contradições e defesas adequadas, oportunizando a recolha de elementos convincentes e fortes para fundamentar o estatuto da condenação” (TAVORA; ALENCAR, 2012, p. 382).

Ciente da existência de tais provas, os legisladores reconheceram que, nos termos do artigo 155 do Código de Processo Penal, os juízes, ao avaliar as provas, podem fundamentar as condenações em provas cautelares, não repetíveis e prospectivas, ainda que surgidas na fase instrutória do processo . A evidência cautelar é que corre o risco de perecer devido à passagem do tempo. Prova não repetível refere-se à prova que não pode ser apresentada novamente devido ao desaparecimento, destruição ou perda da fonte da prova.

Diante do perigo da fragmentação das fontes de prova, uma vez que a autoridade policial toma conhecimento da prática de um crime, pode decidir pela sua prática sem prévia autorização judicial. A evidência prospectiva surgiu devido a circunstâncias exigentes ou relevantes.

Da mesma forma, os atos ilícitos cometidos por meio da tecnologia da informação têm características de boa ocultação e de difícil prova. A ocultação é, na verdade, uma característica inseparável do cibercrime, que se traduz na facilidade com que um programa pode ser modificado de forma a beneficiar o autor e, em seguida, imediatamente modificado novamente para a versão original para cobrir os vestígios deixados pelo invasor. a prática do crime.

Portanto, se a polícia investigar o programa no futuro, não conseguirá descobrir como ocorreu o ato ilícito.

Mesmo permitindo a produção antecipada de provas para crimes virtuais, o procedimento só é eficaz se as provas pertinentes forem essenciais para a condenação futura e houver indícios suficientes de que as provas apresentam risco de perdição. Ainda assim, o programa deve ser analisado contra paradoxos e defesas adequadas para ser eficaz.

5 CONSIDERAÇÕES FINAIS

O objetivo principal do presente trabalho é investigar os crimes cibernéticos de acordo com o Código Penal e Processual Brasileiro, e analisar sob a ótica da legislação estrangeira o impacto desse novo ambiente criminal e as particularidades que dificultam as investigações criminais.

De acordo com a pesquisa, percebe-se que a dificuldade de definir um espaço virtual é facilmente verificada. Em consequência, é difícil definir o cibercrime para avaliação, o que se revela uma tarefa cansativa e difícil, dadas as complexas limitações do seu território, propensão para o anonimato, falta de conhecimento e formação das autoridades de investigação, grande número de pessoas capazes de divulgar tecnologia para esses usos facilita muito a prática de crimes virtuais, além de dificultar o contato com os responsáveis e puni-los.

Após a realização de pesquisas sobre o tema, concluiu-se que é necessário em nosso ordenamento jurídico tipificar imediatamente os crimes cometidos via Internet, pois para combater crimes em ambientes virtuais aplica-se apenas a lei penal, e quase sempre os agentes que cometem tais crimes acabam impunes.

Portanto, diante do exposto, torna-se claro que esses crimes virtuais devem ser regulamentados para que crimes no ambiente virtual não fiquem impunes e causem danos à sociedade. Deve-se lembrar que o direito deve acompanhar as mudanças e transformações da sociedade, adaptar-se à sociedade da informação e ao mundo virtual, zelar pela segurança e garantir a proteção jurídica dos direitos humanos fundamentais.

Concluiu-se que, com o apoio dos computadores, o cibercrime não só leva ao surgimento de novos atos ilícitos, como também possibilita, assim, a violação de interesses legítimos até então não afetados pelos crimes já regulamentados no Brasil. Sistemas jurídicos, como informação, dados e sistemas de computador.

As especificidades na incidência de crimes cibernéticos, como o dinamismo com que esses crimes são cometidos, estão intimamente relacionadas à investigação de provas. Assim, diante da falta de tecnologia e de um quadro humano preparado, surge a importância da especialização dos profissionais que se dedicam a essas investigações.

Além disso, quanto à identificação da autoria, embora seja um tanto fácil rastrear o computador em que ocorreu o crime, é difícil vincular o computador ao sujeito do crime. Para combater isso, propõe-se usar biometria e prender criminosos ativos enquanto o computador estiver ativo.

Por isso, é cada vez mais importante antecipar as instituições produtoras de provas, dada a enorme volatilidade dos meios que serão utilizados como prova para o cibercrime, dado o potencial de desaparecimento de provas.

REFERÊNCIAS

ANDREUCCI, Ricardo Antonio. **Legislação penal especial**. 12ª ed. São Paulo: Saraiva, 2017.

ASSOCIAÇÃO DE EMPRESAS E PROFISSIONAIS DA INFORMAÇÃO. **Brasil sofre mais de 16,2 bilhões de tentativas de ataques cibernéticos na primeira metade de 2021**. 2021. Disponível em: Brasil sofre mais de 16,2 bilhões de tentativas de ataques cibernéticos na primeira metade de 2021 | ABEINFO (abeinfobrasil.com.br). Acesso em: 06 abr 2023.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Brasília, 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm . Acesso em: 10 mai 2023.

BRASIL. **Decreto-Lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Brasília, 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm. Acesso em: 10 mai 2023.

CENTRO DE PREVENÇÃO, TRTAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS DE GOVERNO. **Incidentes**. Disponível em: https://www.gov.br/ctir/ptbr/assuntos/ctir-gov-em-numeros/incidentes . Acesso em: 06 abr 2023.

CERT.br. **Cartilha de Segurança para Internet**. Versão 4.0. São Paulo: Comitê Gestor da Internet no Brasil, 2012. Disponível em: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf. Acesso em: 06 abr 2023.

COLLI, Maciel. Cibercrimes. **Limites e perspectivas à investigação policial de crimes cibernéticos**. Curitiba: Juruá Editora, 2010.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Editora Saraiva, 2011.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011.
CUNHA, Rogério Sanches. **Manual de Direito Penal: Parte Geral**. Salvador: Juspodivm, 2014.

D'URSO, Luiz Augusto Filizzola. **Cibercrime: perigo na internet**. Publicado em 2017. Disponível em: http://politica.estadao.com.br/blogs/fausto-macedo/cibercrime-perigo-na-internet/ Acesso em 05 abr 2023.

EILSTRUP-SANGIOVANNI, Mette. **Why the World Needs an International Cyberwar Convention**. Philosophy Technology, vol 31, p. 379-407, 2018.

EUROPEAN UNION AGENCY FOR CIBERSECURITY. **ENISA Threat Landscape 2021** – April 2020 to mid-July 2021. 2021. Disponível em: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021. Acesso em: 06 abr 2023.

FUTURE. Brasil**: um dos líderes em controle de botnet**. 2017. Disponível em: https://www.future.com.br/blog/brasil-um-dos-lideres-em-controle-de-botnet/. Acesso em: 06 abr 2023.

HERCHEUI, **Magda et al. ICT Critical Infraestructures and Society**. In: IFIP TC 9 International Conference on Human Choice and Computers, 10. ed. Amsterdam, Springer, 2012.
.
INTERPOL. **Cybercrime: Covid-19 Impact**. 2020. Disponível em: https://www.interpol.int/Crimes/Cybercrime/COVID-19-cyberthreats. Acesso em: 06 abr 2023.

JAISHANKAR, Karuppannan. **Establishing a Theory of Cyber Crimes. International Journal of Cyber Criminology**, v. 1, p. 7-9, 2007. Disponível em: http://www.cybercrimejournal.com/Editoriaijccjuly.pdf. Acesso em: 05 abr 2023.

JESUS, Damásio de. MILAGRE, José Antonio. **Manual de Crimes de Informáticos**. São Paulo: Saraiva, 2016.

JESUS, Damasio de; MILAGRE, José Antonio. **Manual de Crimes Informáticos**. São Paulo: Saraiva, 2016.

KHANNA, Pallavi. **State Sovereignty and Self-Defence in Cyberspace**. BRICS Law Journal, New Delhi, vol. 5 (4), p. 139-154, 2018.

LEON, Lucas Pordeus**. Brasil tem 152 milhões de pessoas com acesso à internet**. AgênciaBrasil, Brasília, 2021. Disponível em: Brasil tem 152 milhões de pessoas com acesso à internet | Agência Brasil (ebc.com.br). Acesso em: 06 abr 2023.
LOPES Jr., Aury. **Sistemas de investigação preliminar no processo penal**. Rio de Janeiro: Lumen Juris, 2012.

LOPES, Gills V; NETO, Walfredo B. **A Questão da Fronteira Cibernética no Âmbito das Relações Internacionais Cibernéticas (CiberRI)**. In: Encontro Nacional da Associação Brasileira de Relações Internacionais (ABRI), 5ª edição, 2015.

MALAQUIAS, Roberto Antônio Darós. **Crime Cibernético e Prova – A investigação criminalem busca da verdade**. Curitiba: Juruá Editora, 2012.

MARTINS, **Marco. Ciberespaço: Uma Nova Realidade para a Segurança Internacional.** Revista sobre Cibersegurança do IDN. Lisboa. Nº 133. pp. 32-49. 2012.

MARTINS, Pedro Batista. **Comentários ao Código de Processo Civil**. Forense, v.2, 2017.

NUCCI, Guilherme de Souza. **Manual do Direito Penal**. 7. ed. São Paulo: Revista dos Tribunais, 2011.

NYE, Joseph. **Cyber Power.** Harvard Kennedy School: Belfer Center for Science and International Affairs, Cambridge, p. 1-24, 2010.

PINHEIRO, Patrícia Peck. **Direito Digital**. 4. Ed. São Paulo: Saraiva, 2010.

PINHEIRO, Patrícia Peck. **Direito Digital**. São Paulo: Editora Saraiva, 2013.

PINHEIRO, Patrícia Peck. **Regulamentação da Web**. Cadernos Adenauer XV, Rio de Janeiro, n. 4, p. 33-44, out/2014. Disponível em: < http://www.kas.de/wf/doc/16471-1442-5-30.pdf> Acesso em: 05 abr 2023.

RODRIGUES, Thalita Scharr; FOLTRAN JUNIOR, Dierone César. **Análise de ferramentas forenses na investigação digital**. 2010. Disponível em: http://www.revistaret.com.br/ . Acesso em: 30 mar 2023.

SALTZMAN, Ilai. (2013). **Cyber posturing and the offense-defense balance. Contemporary Security Policy**, 34(1), p. 40–63. 2013.

SANTOS, Liara Ruff dos; MARTINS, Luana Bertasso; TYBUCSH, Francielle Benini Agne. **Os crimes cibernéticos e o direito a segurança jurídica: uma análise da legislação vigente no cenário brasileiro contemporâneo**. 2017.

SEABRA, Miguel P. **O Conceito de Fronteira: Uma abordagem multifacetada. Trabalho de Investigação Individual do Curso de Estado-Maior Conjunto**. Instituto de Estudos Superiores Militares. Portugal, Lisboa, 68f, 2012.

SILVA, Marco Antônio Marques da Silva. **Acesso à Justiça Penal e Estado Democrático de Direito**. São Paulo: Ed. J. de Oliveira, 2011.

SINGER, P.W; FRIEDMAN, Allan. **Cybersecurity and Cyberwar: What Everyone Needs to Know.** 1. ed. Oxford: Oxford University Press, 2013.

SYDOW, Spencer Toth. **Delitos informáticos próprios: uma abordagem sob a perspectiva vitimodogmática**. 2009. Dissertação (Mestrado em Direito Penal) - Faculdade de Direito - Universidade de São Paulo, São Paulo, 2009. Disponível em: http://www.egov.ufsc.br/portal/sites/default/files/delitos_informaticos_proprios_uma_abordagem_sob_a_perspectiva_vitimodogmatica.pdf . Acesso em: 05 abr 2023.
TAVORA, Nestor; ALENCAR, Rosmar Rodrigues. **Curso de Direito Processual Penal**. Salvador: Jus Podivm, 2012.

THE HARRIS POLL. 2021 **Norton cyber safety insights report global results**. 2021. Disponível em: https://now.symassets.com/content/dam/norton/campaign/NortonReport/2021/2021_NortonLi feLock_Cyber_Safety_Insights_Report_Global_Results.pdf. Acesso em 06 abr 2023.

TOLEDO, Marcelo. **Hackers invadem sistema do Hospital do Câncer de Barretos e pedem regaste**. Publicado em 2017. Disponível em : https://www.em.com.br/app/noticia/internacional/2017/05/12/interna_internacion Acesso em: 05 abr 2023.

VIANNA, Túlio Lima. **Dos crimes pela internet**. Disponível em: http://www.academia.edu/1911162/Dos_crimes_pela_internet. Acesso em: 05 abr 2023.

WEBER. **Livros Técnicos e Científicos S.A**, Rio de Janeiro, 5ª ed, 1982. Disponível em:. Acesso em: 15 de março de 2020.

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