FACULDADES INTEGRADAS DE PONTA PORÃ

GLEYCE ORTIZ MINHO

CRIMES CIBERNÉTICOS SOB A LEGISLAÇÃO PENAL BRASILEIRA:

O ESTELIONATO VIRTUAL

PONTA PORÃ

2021

GLEYCE ORTIZ MINHO

CRIMES CIBERNÉTICOS SOB A LEGISLAÇÃO PENAL BRASILEIRA: O ESTELIONATO VIRTUAL

Trabalho de Curso – TC apresentado à Banca Examinadora das Faculdades Integradas de Ponta Porã, como exigência parcial para obtenção do título de Bacharel em Direito.

Orientadora: Prof.ª, Esp. Renata Freitas de Souza.

PONTA PORÃ

2021

GLEYCE ORTIZ MINHO

CRIMES CIBERNÉTICOS SOB A LEGISLAÇÃO PENAL BRASILEIRA: O ESTELIONATO VIRTUAL

Trabalho de Curso – TC apresentado à Banca Examinadora das Faculdades Integradas de Ponta Porã, como exigência parcial para obtenção do título de Bacharel em Direito.

Orientadora: Prof.ª, Esp. Renata Freitas de Souza.

Banca Examinadora

_____

Profª Esp. Renata de Freitas Souza
Faculdades Integradas de Ponta Porã – FIP

_____

Professor(a) avaliador(a)
Faculdades Integradas de Ponta Porã – FIP

_____

Professor(a) avaliador(a)
Faculdades Integradas de Ponta Porã – FIP

Ponta Porã, _____de _____ de 2021.

“É muito melhor lançar-se em busca de conquistas grandiosas, mesmo expondo-se ao fracasso, do que alinhar-se com os pobres de espírito, que nem gozam muito nem sofrem muito, porque vivem numa penumbra cinzenta, onde não conhecem nem vitória, nem derrota.” (Theodore Roosevelt)

AGRADECIMENTOS

Primeiramente á Deus, por me dar sabedoria, e principalmente forças prosseguir todas as vezes que pensei em desistir.

Á minha mãe Rita, que sempre me incentivou e me serve de inspiração para prosseguir nas lutas diárias.

Á meu pai Mário, que sempre me apoiou e sonha comigo todas as coisas que desejo.

Á minha irmã Gabriela, pelo amor, incentivo e apoio.

Á meu esposo Cleiton, por me acompanhar todos esses cinco anos diariamente e não me deixar desistir nunca.

Aos meus parentes, maternos e paternos que acreditam no meu crescimento.

Aos amigos de Faculdade, Caroline e Rosemir, por caminharmos juntos durante todo o curso.

Aos colegas da Polícia Civil de Coronel Sapucaia, pela aprendizagem adquirida nos quatro anos de estágio.

RESUMO

O presente trabalho tem como objetivo analisar os crimes praticados no âmbito virtual. Com o auxílio da doutrina e legislação recente, o intuito é estudar o delito de estelionato virtual bem como os procedimentos de investigação utilizados para descobrir a autoria e garantir a repressão e punibilidade dos crimes cibernéticos, analisando se estes mecanismos são realmente eficazes no combate á criminalidade virtual. Considerando que a internet vem crescendo em uma velocidade acelerada no país e a cada dia os cidadãos se familiarizam mais com os recursos tecnológicos é necessário discutirmos sobre o assunto, visto que, juntamente com seus benefícios a internet também traz riscos. Este crescimento desordenado da tecnologia e da internet são os principais fatores que fizeram com que os crimes cibernéticos sofressem alta. Diante disso, surge à necessidade da criação de normas que regulem essas relações, mantenham a ordem e protejam os bens jurídicos tutelados pelo ordenamento jurídico. Sendo assim, ocorrerá uma dissertação sobre os crimes cibernéticos, desde sua historicidade até seus aspectos gerais e específicos, também serão abordadas disposições acerca do estelionato virtual e ainda, os procedimentos adotados na investigação e consequentemente punibilidade dos autores dos delitos, bem como se estes mecanismos realmente surtem efeitos. Para tanto, serão utilizadas pesquisas bibliográficas, as quais consistem na leitura, análise e fichamento de doutrinas e artigos científicos que versem sobre o tema.

Palavras-chave: internet; crimes cibernéticos, estelionato virtual; investigação e punibilidade.

ABSTRACT

This work aims to analyze crimes committed in the virtual environment. With the help of recent doctrine and legislation, the aim is to study the crime of virtual embezzlement as well as the investigation procedures used to discover the authorship and ensure the repression and punishment of cyber crimes, analyzing whether these mechanisms are really effective in fighting crime virtual. Considering that the internet has been growing at an accelerated speed in the country and citizens are becoming more familiar with technological resources every day, it is necessary to discuss the matter, since, along with its benefits, the internet also brings risks. This disorderly growth of technology and the internet are the main factors that have made cybercrime soar. Therefore, there is a need to create rules that regulate these relationships, maintain order and protect the legal assets protected by the legal system. Thus, there will be a dissertation on cyber crimes, from their historicity to their general and specific aspects, provisions on virtual embezzlement will also be addressed, as well as the procedures adopted in the investigation and consequently the punishability of the perpetrators of the crimes, as well as whether these mechanisms really have effects. Therefore, bibliographical research will be used, which consist of reading, analyzing and listing scientific doctrines and articles that deal with the topic.

Keywords: internet; cyber crimes, virtual embezzlement; investigation and prosecution.

LISTA DE ILUSTRAÇÕES

GRÁFICOS

TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ARPA- Research Projects Agency

MINICON- Ministério das Comunicações

EMBRATEL- Empresa Brasileira de Telecomunicações

RENPAC- Rede Nacional de Pacotes

LNCC- Laboratório Nacional de Computação Científica

FAPESP- Fundação de Amparo á Pesquisa de São Paulo

UFRJ- Universidade Federal do Rio de Janeiro

UNAN- Faculdade de Direito da Universidade Nacional Autônoma do México

OECD- Organização para a Cooperação Econômica e Desenvolvimento

CPI- Comissão Parlamentar de Inquérito

EMBRAPA- Empresa Brasileira de Agropecuária

SEJUSP- Secretária de Estado de Justiça e Segurança Pública

DI- Delegacia Interativa

PCDF- Polícia Civil do Distrito Federal

IP- *Internet Protocol*

SUMÁRIO

INTRODUÇÃO

A informação é um dos pilares do convívio social. Em decorrência dos avanços tecnológicos a população em geral classifica como indispensável o acesso à informação. Diferentemente dos séculos XVIII e XIX, em que a grande maioria das notícias do Brasil e do mundo eram transmitidas através do rádio e da televisão, atualmente, existe um mecanismo de informação muito mais sofisticado, a internet.

A internet é uma das invenções mais incríveis já desenvolvidas pelo homem, visto que, esta ferramenta está em constante transformação, possibilitando a realização de diversos afazeres através de um aparelho eletrônico conectado á rede. Além de compartilhar notícias, muitas outras funções podem ser exercidas através desta rede. Pode-se dizer que hoje a internet cumpre um papel essencial na vida do ser humano e este se torna cada vez mais dependente dela.

Muitos são os benefícios trazidos das inovações tecnológicas. A familiarização das pessoas com a tecnologia faz com que está esteja sempre inovando e se adaptando as novas necessidades das relações sociais. Os recursos tecnológicos estão facilitando a realização de atividades do cotidiano que atualmente passam a ser executadas do conforto de casa.

No entanto, a criminalidade digital cresce juntamente com esta revolução tecnológica. Em decorrência disto, se faz necessário mencionar os riscos advindos da informatização em massa, pois, além dos benefícios, há muitos males trazidos pela internet, os quais são desconhecidos por um número considerável de usuários.

O âmbito virtual atrai diversos criminosos que enxergam a rede como um local apropriado para o cometimento de crimes, já que, através do uso de recursos tecnológicos é muito fácil manter o anonimato e consequentemente a impunidade pelos delitos que cometerem neste território. Dai surge o assunto da presente pesquisa, os crimes cibernéticos.

São chamados de crimes cibernéticos os delitos cometidos por meio de aparelhos eletrônicos conectados à rede. Em decorrência da evolução desse tipo de crime, o Direito também necessitou evoluir, já que é o responsável por regular os conflitos derivados das relações mantidas pela sociedade.

Muitas são as possibilidades de cometimento de crimes pela internet, os exemplos mais comuns, são: a pornografia infantil, invasão de privacidade, crimes

contra a honra e o estelionato. O estelionato virtual é o delito ao qual será dado uma atenção especial na presente.

Com o advento da Lei nº 14.155\2021, a fraude eletrônica ganhou um espaço na legislação, já que antes não possuía um dispositivo específico que tratava da punibilidade deste respectivo crime. O art. 171 do Código Penal recebeu dois novos parágrafos. Além destes novos parágrafos, foram efetuadas modificações e incorporações de novas disposições em outros artigos, os quais passaram a dispor de uma punibilidade mais severa. Vale ressaltar ainda, que o Código de Processo Penal também sofreu alteração pela referida lei.

A Lei 14.155\2021 foi um divisor de águas para o Direito Penal, já que agora no Código Penal Brasileiro há uma observância maior no que se refere aos crimes cometidos no âmbito virtual. Não menos importantes são as leis que já existiam e tratavam de delitos praticados pela rede, uma das mais conhecidas é a Lei nº 12.737\2012 apelidada como “Lei Carolina Dieckmann”, a qual trata do delito de invasão de dispositivo informático e que também sofreu alteração pela nova lei.

Observa-se que a problemática não está mais concentrada na falta de tipificação dos delitos no ordenamento jurídico, mas sim, na dificuldade que o Poder Judiciário enfrenta em estabelecer a correta identificação do criminoso e aplicar a sanção penal. Na fase das investigações são encontrados diversos obstáculos, como, a dificuldade na obtenção de provas e a necessidade de perícia especializada, os quais contribuem para a não identificação dos autores dos crimes virtuais.

Sem dúvidas, as tecnologias, juntamente com a internet, estão quebrando fronteiras, e isso, é excelente para o desenvolvimento e avanço mundial, no entanto, devem ser reconhecidas a periculosidade dessas ferramentas e a carência de efetividade das normas que visam punir os sujeitos causadores de danos aos bens tutelados pelo ordenamento jurídico.

Para tratar dos temas brevemente mencionados acima, a pesquisa está estrutura em três capítulos. O primeiro capítulo ira abordar as noções introdutórias sobre crimes cibernéticos, como o nascimento da internet, bem como sua chegada ao Brasil, a relação entre o Direito e a informática, conceitos relativos aos crimes cibernéticos, suas classificações e ainda, o surgimento dos primeiros crimes virtuais e o crescimento da ilicitude em rede.

O segundo capítulo irá tratar do crime de estelionato virtual e sua previsão legal no ordenamento jurídico brasileiro. Inicialmente far-se-á uma introdução à teoria do

crime, para que seja compreendida a sanção penal imposta pelo Estado aos agentes que violam as normas jurídicas. Após isso, serão dispostas observações a respeito do crime de estelionato comum, previsto no art. 171 do Código Penal, e posteriormente, serão traçadas considerações gerais do crime de estelionato virtual, bem como as alterações trazidas pela Lei nº 14.155\2021 a respeito do citado delito, tanto no Código Penal, como no Código de Processo Penal.

O terceiro capítulo será destinado a tratar das dificuldades na aplicabilidade da legislação. Os aspectos abordados no presente remetem-se a complexidade em se estabelecer de fato quem é o autor do crime cibernético e os obstáculos enfrentados na fase das investigações. Descobrir a autoria de fato não é tarefa fácil, a rede é um local obscuro no qual é possível valer-se do anonimato para acessa-la, e ainda quando identificado, pode ser que não seja sua identificação pessoal, mas sim de terceiros. Diante disso, serão necessários reunir conjuntos probatórios, e ainda, pode surgir a necessidade de realização de perícia especializada. Dadas às informações introdutórias, estes assuntos serão aprofundados dentro do terceiro capítulo.

Por fim, o quarto capítulo, de forma breve irá dispor de considerações a respeito da Convenção sobre crime cibernético, conhecida também como Convenção de Budapeste. A mencionada é o primeiro tratado internacional sobre crimes virtuais e atualmente está aguardando a aprovação do Senado Federal para incorporar-se a legislação brasileira.

Nas considerações finais restam as conclusões acerca das pesquisas realizadas e descritas.

1. CRIMES CIBERNÉTICOS

Antes de proceder à análise aprofundada na problemática do tema apresentado, cumpre suceder uma historicidade do crime cibernético, para tanto, se faz necessário expor alguns pontos essenciais. Inicialmente serão descritos o histórico da internet, a relação entre o Direito e a informática, a conceituação de crimes cibernéticos, sua classificação, e por fim, o surgimento dos primeiros crimes virtuais, bem como o avanço da ilicitude em rede.

Concluída está pequena introdução, proximamente iremos adentrar mais especificamente no crime de estelionato virtual previsto no Código Penal Brasileiro, no entanto, para se chegar á um assunto mais específico é necessário que o leitor possua conhecimento dos seus antecedentes históricos.

1.1. O NASCIMENTO DA INTERNET E A IMPLANTAÇÃO NO BRASIL

No ano de 1945, findada a Segunda Guerra Mundial, a tecnologia sofre avanço significativo e o mundo habitua como indispensável à comunicação rápida e globalizada (FUCHS; STUANI, 2021). Diante das disposições a seguir, iremos observar que a chegada do Homem á Lua, apesar de ser um grande marco histórico, decai do lugar de maior evolução mundial com o surgimento da primordial rede de comunicações, a internet (VIEIRA, 2003).

O Departamento de Defesa dos Estados Unidos, por meio de um grupo de pessoas capacitadas, engenheiros e programadores eletrônicos, elaboraram uma rede de comunicações sem que houvesse nenhum controle central. Com isso, a comunicação dos centros de pesquisas e as bases das Forças Armadas seriam efetuadas de forma mais rápida e flexível (VIEIRA, 2003).

Em meados dos anos 60, essa rede começou a ser desenvolvida com o objetivo de facilitar a comunicação entre os militares, principalmente em tempos de guerra. Esse sistema deveria suportar qualquer tipo de ataque, inclusive, um possível conflito nuclear. Dessa premissa surge a ideia de que a internet nasceu das mãos dos militares norte-americanos, já que, os mesmo acreditavam que um meio de comunicação mais eficaz, seria capaz de fazê-los vencer uma guerra (VIEIRA, 2003).

A Research Projects Agency (ARPA), órgão responsável, para fins militares, pelas pesquisas científicas e tecnológicas foi quem financiou o Projeto, o qual veio a

ser batizado como Arpanet (VIEIRA, 2003). Essa idealização ganhou força em meio à tensão da Guerra Fria, e foi um marco histórico para os Estados Unidos, já que anos mais tarde se tornou a ferramenta de comunicação mais importante já desenvolvida pelo homem (FUCHS; STUANI, 2021).

O projeto obteve êxito, e a primeira conexão a rede ocorreu em janeiro de 1972, onde quatro computadores distintos, todos norte-americanos se interligaram, e os mesmos puderam enviar e receber mensagens. Em 1974, a Arpanet estabeleceu a conexão entre cem computadores, os quais cresceram expressivamente, o que contribuiu para que a rede saísse do âmbito acadêmico e impressionasse o mundo (VIEIRA, 2003).

No ano de 1988 o Brasil teve uma das suas primeiras experiências com a conexão à internet (CARVALHO, ARITA, NUNES). No entanto, vale ressaltar que anteriormente já havia despertado o interesse do setor de telecomunicações nacional, o qual foi responsável pela sociabilidade da internet no país.

Comandado pelo Poder Público, o setor de telecomunicações possuía inicialmente dois objetivos com essa nova rede: o primeiro, semelhante aos Estados Unidos, era aperfeiçoar a rede de telecomunicações e utiliza-la em estratégias militares com o intuito de garantir a Segurança Pública e o segundo estava ligado a questões financeiras. (BENAKOUCHE, 1997).

Segundo Benakouche (1997, p. 126) a ala nacionalista do governo enxergou uma oportunidade com a implantação dessa nova tecnologia no país:

> [...] ala nacionalista do governo, que sonhava com um “Brasil, Grande Potência”; seus representantes viam nas inovações tecnológicas incorporadas àquelas redes oportunidades para o desenvolvimento da então inexpressiva indústria local de telecomunicações e para a criação de uma estrutura nacional de Pesquisa e Desenvolvimento (P&D).

O uso de equipamentos informáticos se expandiu no ano de 1975, deixando totalmente claro a convergência existente entre as tecnologias de comunicação e a informática. (BENAKOUCHE, 1997) Derivado deste acontecimento, estudos foram colocados em prática, para que ambos os ramos caminhassem paralelamente.

Ainda no ano 1975, o Ministério das Comunicações (MINICOM) atentou-se a assuntos relacionados à transmissão eletrônica de dados, denominada na época de telemática ou teleinformática, para tanto, elaborou o decreto nº 301 que determinava

que a Empresa Brasileira de Telecomunicações (Embratel) seria a responsável por instalar e explorar a transmissão eletrônica de dados. (CARVALHO, ARITA, NUNES).

Cinco anos mais tarde, em maio de 1980, o decreto 104 funda a Transdata, a qual passa a ser alugada para os grandes consumidores de transmissão de dados. Conforme Benakouche (1997, p. 128):

> Essa rede era constituída por circuitos privados do tipo ponto-a-ponto (não comutados, portanto), alugados pela Embratel a preços fixos, calculados com base na distância que separava os correspondentes e na velocidade da transmissão (medida em bites por segundo/bts).

Com os mesmos fins que a Transdata, em 1985, é desenvolvida uma nova rede, a Renpac (Rede Nacional de Pacotes). De natureza pública, nas palavras de Benakouche (1997) é destinada ao chamado “grande público”. Em dois anos de funcionamento está rede captou cento e dez assinantes, o que não era bom, já que havia atraído um número muito baixo de usuários (CARVALHO, ARITA, NUNES).

A Renpac seria a responsável por tornar a rede pública de transmissão de dados em um sistema de uso doméstico, no entanto, como já esperado pela Embratel, não obteve sucesso. Ante ao fracasso do projeto, surge à necessidade de por em prática um plano B, o projeto cirandão (BENAKOUCHE, 1997).

O cirandão, já desenvolvido anteriormente pela Embratel e denominado ciranda, possuía como finalidade capacitar os funcionários da própria empresa no uso de computadores, já que a área para qual prestavam serviços exigia mão de obra especializada em técnicas digitais (BENAKOUCHE, 1997).

Em 1988, o Laboratório Nacional de Computação Científica (LNCC) financiado pelo CNPq, realizou a primeira conexão com o exterior, utilizando a Renpac se conectou a rede norte-americana Bitnet. Neste mesmo ano, a Fundação de Amparo á Pesquisa de São Paulo (Fapesp), se conectou com duas redes, a Bitnet e a Hepnet, demonstrando assim, a ânsia da instituição brasileira sob a Internet. A Universidade Federal do Rio de Janeiro (UFRJ), em 1989, estabeleceu uma terceira conexão internacional no país, conectando-se também com a Bitnet (CARVALHO, ARITA, NUNES).

Decorrido dois anos do início da internet no país, no final de 1991, a rede executada pelas instituições acadêmicas havia crescido expressivamente, no entanto, possuía custo elevado, já que era necessário pagamento de taxas, como o aluguel da

rede e impulsos telefônicos, diante disso, foi criado um projeto para construção de uma infraestrutura em forma de malha (CARVALHO, ARITA, NUNES).

“O rápido desenvolvimento da rede no mundo já demonstrava aos vários setores da sociedade o potencial deste sistema de comunicação de dados” (CARVALHO, ARITA, NUNES). Neste contexto, diversos projetos foram desenvolvidos e aperfeiçoados, para se chegar à imensidão que se tornou a internet nos dias atuais.

1.2. O DIREITO E A INFORMÁTICA

Um dos alicerces sociais de forma globalizada é a informação, a qual é vista como combustível para o desenvolvimento e bem estar da sociedade. A informação é utilizada com o intuito de proporcionar melhor qualidade de vida, facilidade de comunicação e integração social. Além disso, oportuniza conhecimento, o que faz com que a sociedade esteja em constante transformação (JESUS, MILAGRE, 2016).

A tecnologia atualmente é uma das responsáveis pelas mutações sociais. Inseparável desta sociedade é o acesso às tecnologias. Estar conectado à rede passou a ser um direito de todos e é através desta ferramenta que as pessoas se comunicam, sem ao menos saber como, para onde e quais os riscos que isto oferece (JESUS, MILAGRE, 2016).

O Direito foi um dos ramos atingidos por esse crescimento expressivo das tecnologias, em razão disso, surgiu à necessidade de serem desenvolvidos estudos com o intuito de implantar novos modelos legislativos para sanar os problemas advindos do uso em massa dessa nova tecnologia (SILVA, 2003).

O Direito da informática surge exatamente dessa revolução tecnológica, e conforme Silva (2003, p. 41) pode ser conceituado como: “o conjunto de leis, normas e princípios aplicáveis aos fatos e atos decorrentes do tratamento automatizado da informação”.

Uma enorme lição é preconizada por um brocardo antigo: “*ubi societas, ibi jus* (onde está à sociedade está o Direito)” (REALE, 2002, p.18), ou seja, em toda e qualquer relação estabelecida entre a sociedade, estará presente o Direito. Sergio Cavalieri Filho (2019, p. 20) diz que o Direito “está ligado à ideia de organização e conduta social, por isso deve ser concebido como um conjunto de normas de conduta que disciplinam as relações sociais”.

A comunicação digital é exercida por meio do ciberespaço no qual circula diversas informações e por meio do qual é possível exercer atividades do cotidiano (LEVY, 1999). Nota-se que esse espaço digital evolui e potencializa-se gradativamente e atividades que eram exercidas apenas de forma presencial estão sendo simplificadas para serem realizadas de forma remota.

Os recursos tecnológicos estão possibilitando aos seus usuários comodidade, já que apenas com cliques, do conforto de sua casa é possível realizar uma transação bancária, por exemplo, ou até mesmo atividades laborais, estudos ou encontros com amigos por meio de aplicativos de chamadas de vídeo. Essa implantação tecnológica no cotidiano das pessoas deu origem aos bens informáticos, direitos, deveres e limitações de cada usuário desse espaço virtual.

Não há duvidas de que a informática está quebrando barreiras, por isso, devemos reconhecer a carência de normas regulamentares, que previnam, reprimam e punam os fatos ofensivos á ordem jurídica.

O Direito e a informática estão sintonizados, ou seja, um necessita do outro. Conforme Silva (2003), o Direito Penal se relacionada de três formas com a informática, a primeira e a segunda concerne na informatização de documentos e processos penais e administrativos, o que facilita o armazenamento de dados e coopera com a melhoria e a efetividade do trabalho exercido pelo Poder Judiciário, o terceiro modo de se relacionar não é exercido de forma positiva, já que é o uso da informática a serviço da delinquência, ou seja, a informática de certa forma contribui com esses criminosos que se aproveitam do anonimato para tirar vantagem indevida.

Interessa-nos conhecer sobre a informática a serviço de práticas ilícitas, já que atualmente inúmeras ações são executadas através da rede e essas condutas geralmente afetam bens jurídicos tutelados pela norma, como a privacidade, a honra e o patrimônio.

1.3. CONCEITO DE CRIMES CIBERNÉTICOS

Conceituar crimes cibernéticos não é uma tarefa fácil, visto que, as tecnologias são muito amplas, e, além disso, os crimes cibernéticos ainda estão ganhando espaço tanto na doutrina como na legislação, portanto não é pacífica a conceituação do referido delito.

O crime cibernético possui várias nomenclaturas, dentre elas, conforme expõem diversos doutrinadores como Rossini (2004) e Silva (2003), podem ser denominados também crimes informáticos, crimes por computador, crimes de informática, abusos de informática, crimes de computação, delinquência informática, fraude informática, criminalidade do computador, delitos informáticos, entre outros.

Ante aos problemas terminológicos enfrentados, Silva (2018) leciona que crimes informáticos são gênero do qual crimes cibernéticos são espécie, e a grande diferença entre eles é que apesar de serem cometidos através da utilização de um computador, os crimes cibernéticos são consumados no âmbito ou por meio da internet. Para efeitos desse trabalho, será usado o termo “crime cibernético”.

Cumpre destacar que crime sob o aspecto formal é todo fato típico, antijurídico e culpável (JESUS, 2020). A principal diferença de um crime comum para um crime cibernético é justamente a forma de execução. Conforme, já disposto anteriormente, o crime cibernético é executado através de um dispositivo tecnológico e por meio da utilização da internet.

Ivete Senise Ferreira conceitua crimes informáticos como: “toda ação típica, antijurídica e culpável cometida contra ou pela utilização de processamento automático de dados ou sua transmissão” (apud ROSSINI, 2004, p. 104). De semelhante modo, numa definição clássica de crimes informáticos Daoun atribui o seguinte conceito: “toda a ação típica, antijurídica e culpável com o adendo de ser cometido contra ou pela utilização de sistemas informáticos ou informatizados” (apud, SILVA, p. 56).

Já Reginaldo César Pinheiro define crimes informáticos como: “toda conduta positiva ou negativa (ação ou omissão), praticada total ou parcialmente no ambiente informático e que venha a causa um prejuízo à vítima, seja ele patrimonial ou não” (apud ROSSINI, 2004, p. 105).

Rossini (2004, pág. 110) define crimes informáticos como:

> “Conduta típica e ilícita, constitutiva de crime ou contravenção penal, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem elementos a integridade, a disponibilidade e a confiabilidade”.

Para Jesus e Milagre (2016, p. 48) “crime informático é um fenômeno inerente às transformações tecnológicas que a sociedade experimenta e que influenciam

diretamente no Direito Penal". De forma mais simples e concreta é todo o fato típico e antijurídico cometido por meio da ou contra a tecnologia da informação.

Maria de La Luz Lima preconiza que crime informático é "qualquer conduta criminógena ou criminal que em sua realização faz uso da tecnologia eletrônica seja como método, meio ou fim e que, em um sentido estrito". (apud ROSSINI, 2004, p. 105).

A Faculdade de Direito da Universidade Nacional Autônoma do México (UNAN), definiu os delitos informáticos como: "todas aquelas condutas ilícitas suscetíveis de ser sancionadas pelo Direito Penal, que fazem uso indevido de qualquer meio informático." (apud ROSSINI, 2004, p. 106).

Importante destacar que Jesus e Milagre (2016, p. 49) fazem menção na doutrina a respeito de uma distinção entre delitos informáticos e criminalidade na Internet:

> "Rodríguez Mourullo, Alonso e Lascuraín (apud FERREIRA, 2004, p. 52), ao tratarem de crimes informáticos, apresentam interessante distinção: os delitos informáticos teriam como objeto de ataque um elemento informático, ou seja, dados e/ou sistemas informáticos, enquanto a criminalidade na Internet seria o instrumento do delito".

A Organização para a Cooperação Econômica e Desenvolvimento (OECD), na década de 90, reconheceu como crime informático "qualquer conduta ilegal, não ética, ou não autorizada, que envolva processamento automático de dados e\ou a transmissão de dados" (SILVA, 2003, p. 55).

Diversas são as definições atribuídas aos crimes ou delitos informáticos. Os conceitos mencionados podem ser considerados como definição de crime cibernético, embora alguns se destaquem todos se remetem a ele. Analisados os conceitos prescritos acima, conclui-se que, crime cibernético é toda aquela conduta típica, ilícita e culpável, na qual o sujeito utiliza-se de dispositivos e recursos informáticos conectados a internet ou por meio dela para obtenção de vantagem ilícita ou acesso indevido.

1.4. CLASSIFICAÇÃO DOS CRIMES CIBERNÉTICOS E BREVES CONSIDERAÇÕES A RESPEITO DO SUJEITO ATIVO

Classificações concernentes aos crimes cibernéticos foram estabelecidas por doutrinadores estrangeiros, dentre elas, as mais conhecidas são as definidas pelo alemão Klaus Tiedemann, por Ulrich Sieber e pela francesa Martine Briat. Os doutrinadores brasileiros não ficaram para traz, pois, também criaram suas classificações, cada um de acordo com seu entendimento (JESUS, MILAGRRE, 2016).

Marco Aurélio Rodrigues da Costa classifica o delito como crime de informática puro, crime de informática misto e crime de informática comum. Segundo ele:

> "Crimes de informática puros são aqueles em que o sujeito ativo visa especificamente ao sistema de informática, em todas suas formas [...] toda e qualquer conduta ilícita que tenha por objetivo exclusivo o sistema de computador, seja pelo atentado físico ou técnico do equipamento e seus componentes, inclusive dados e sistemas. Os crimes de informática mistos são todas aquelas ações em que o agente visa a um bem juridicamente protegido diverso da informática, porém o sistema de informática é a ferramenta indispensável para sua consumação. Crimes de informática comum: são todas aquelas condutas em que o agente se utiliza d sistema de informática como mera ferramenta á perpetração de crime comum, tipificável na lei penal." (apud, ROSSINI, 2004, p. 119).

Viana e Machado (2013) classificam os crimes informáticos em: impróprios, próprios, mistos e mediatos ou indiretos:

> As condutas típicas nas quais o computador serviu como instrumento para a execução de um crime, mas não houve ofensa ao bem jurídico inviolabilidade da informação automatizada (dados), serão denominadas de *crimes informáticos impróprios*. Já os crimes em que há a infringência à inviolabilidade da informação automatizada serão chamados de *crimes informáticos próprios*. Os crimes complexos, em que, além da proteção à inviolabilidade dos dados, a norma visar a tutela de bem jurídico diverso, serão denominados *crimes informáticos mistos*. Por fim, nos casos em que um delito informático próprio é praticado como crime-meio para a realização de um crime-fim não informático, este acaba por receber daquele a característica de informático, razão pela qual o denominaremos de *crime informático mediato* ou *indireto*.

Jesus e Milagre (2016) também classificam crimes informáticos de modo semelhante ao disposto por Viana e Machado, assim, podemos observar que diversos são os doutrinadores e as classificações estabelecidas por eles. O intuito dessas classificações é justamente categorizar bem os crimes cibernéticos e demonstrar de forma ampla a possibilidade de utilização dos meios informáticos para o cometimento de delitos e consequentemente prejuízo a bens jurídicos tutelados pela legislação penal.

No que concerne ao sujeito ativo do delito é comum utilizar a expressão *hacker,* no entanto, é preferível a denominação *cracker,* pois, tal demonstra mais tecnicidade. Observe:

> *Hacker* refere-se aquele sujeito [...] capaz de entrar e sair de um computador sem que se perceba, mostrando-se como verdadeiro especialista. [...] *Cracker* é o invasor destrutivo que tenta invadir na surdina portões de entrada dos servidores internet, que são a melhor forma de disseminar informações (SILVA, 2003, p. 78).

Na Comissão Parlamentar de Inquérito (CPI) destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país, foram citadas outras figuras, sujeitos ativos do referido delito, os desenvolvedores e os produtores:

> Desenvolvedores são criminosos que se dedicam propriamente à construção das ferramentas computacionais utilizadas para a prática de ilícitos no ciberespaço. Em geral esses criminosos vendem ou alugam suas ferramentas para o grupo dos operadores utilizando a própria internet, por vezes se valendo até mesmo de mídias sociais como o Facebook para divulgar seus “serviços” e “produtos”. Já os operadores são aqueles que utilizam as ferramentas computacionais para o efetivo cometimento dos crimes cibernéticos. Neste ponto, cumpre mencionar que, tipicamente, uma investigação policial bem-sucedida redunda no desbaratamento de um grupo de operadores de crimes cibernéticos, sendo muito raro que se consiga chegar aos desenvolvedores das ferramentas [1].

Além das citadas acima, muitas outras denominações e especificações são dadas aos sujeitos ativos dos crimes cibernéticos, no entanto, não cumpre ao presente delongar-se sobre o assunto. Para finalizar, cumpre ressaltar que, atualmente qualquer pessoa que possui um pouco de conhecimento dos meios tecnológicos é meramente capaz de cometer crimes virtuais, como comumente ocorre na prática do estelionato virtual, o qual não necessita de mão de obra especializada dos autores. Na verdade, pode-se dizer que na rede existem dois tipos de criminosos: os profissionais e os amadores (FLORIANO, RODRIGUES, 2017).

---

[1] CÂMARA DOS DEPUTADOS (Brasil). Congresso Nacional. CPI - Crimes cibernéticos: comissão parlamentar de inquérito destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país. Brasília: 2016. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=214D61B364D3F74027CAB7F56C3E0C39.proposicoesWeb2?codteor=1455189&filename=REL+4/2016+CPICIBER+%3D%3E+RCP+10/2015. Acesso em: 15\11\2021.

1.5. O CRESCIMENTO DA ILICITUDE EM REDE

O surgimento dos primeiros crimes praticados no âmbito da internet se deu por volta da década de 70, sendo grande parte deles realizados por especialistas no ramo da informática, geralmente contra instituições financeiras com a finalidade de obter vantagem ilícita [2].

Os crackers foram os primeiros a der início nas ações criminosas praticadas no âmbito virtual no Brasil (ROSSINI, 2004). Tem-se registro de que a EMBRAPA (Empresa Brasileira de Agropecuária) foi quem sofreu o primeiro ataque no país tendo os seus sistemas computacionais destruídos o que lhes causou grandes prejuízos. O Banco Central, instituição financeira considerada a principal do país também foi atingida pelas ações dos criminosos, o que o levou a quebra, já que mantiveram mais de mil contas fictícias sem que a auditoria do próprio banco notasse este fato [3].

Se houve falar muito dos benéficos trazidos pela tecnologia e o acesso à internet, no entanto, se faz necessário mencionar os riscos advindos da sociedade informatizada. Não são todos os cidadãos que utilizam a internet de boa-fé, existem aqueles que querem tirar aproveitar do fato do seu rosto estar encoberto atrás de uma ferramenta digital para obter vantagens indevidas, dando origem, a chamada criminalidade digital (JESUS, MILAGRE, 2016).

A internet sofreu um avanço considerável se tornando capaz de criar costumes e impor regras na vida de diversas pessoas. (JESUS, MILAGRE, 2016). As redes sociais possuem uma influência tão grande sobre seus telespectadores que os fazem consumirem produtos e serviços oferecidos pelos famosos influenciadores digitais.

Uma pesquisa realizada pelo IBGE em 2019 constatou que 87,7% dos domicílios brasileiros possuem acesso à internet, conforme o gráfico abaixo [4]:

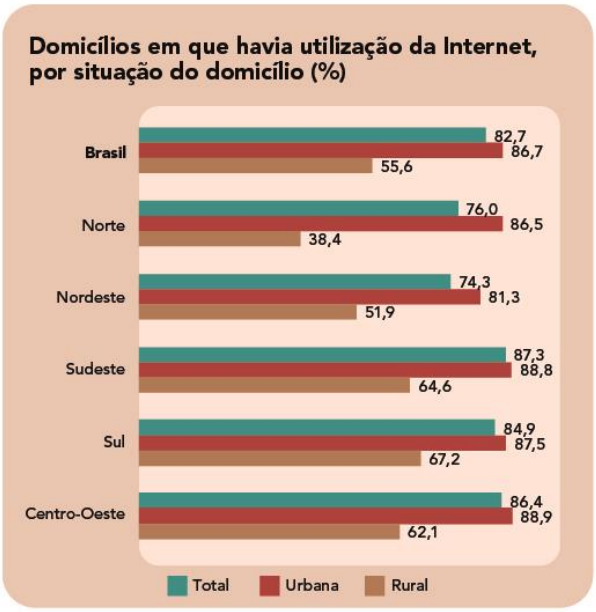
---

[2] Advocacia Direito Digital e Crimes Cibernéticos. Primeiros casos interessantes de crimes na internet. JusBrasil. Disponível em: https://fernandocbrizola.jusbrasil.com.br/artigos/393077456/primeiros-casos-interessantes-de-crimes-na-internet. Acesso em: 15\11\2021.

[3] Advocacia Direito Digital e Crimes Cibernéticos. Primeiros casos interessantes de crimes na internet. JusBrasil. Disponível em: https://fernandocbrizola.jusbrasil.com.br/artigos/393077456/primeiros-casos-interessantes-de-crimes-na-internet. Acesso em: 15\11\2021.

[4] Uso de internet, televisão e celular no Brasil. IBGE Educa Jovens. Disponível em: https://educa.ibge.gov.br/jovens/materias-especiais/20787-uso-de-internet-televisao-e-celular-no-brasil.html. Acesso em: 25\10\2021.

- Gráfico 1- Domicílios em que havia utilização da internet, por situação do domicílio (%)



Fonte: IBGE, Diretoria de Pesquisas, Coordenação de Trabalho e Rendimento, Pesquisa Nacional por Amostra de Domicílios Contínua 2019.

A seguinte tabela demostra os aparelhos mais utilizados para acessar a internet, sendo que, em primeiro lugar está o celular, observe:

- Tabela 1- Equipamentos utilizados para acessar a internet

Fonte: IBGE, Diretoria de Pesquisas, Coordenação de Trabalho e Rendimento, Pesquisa Nacional por Amostra de Domicílios Contínua 2018/2019.

A pandemia do coronavírus (COVID-19) [5] que se propagou no ano de 2020 e perdura até os dias de hoje, mudou a rotina de milhares países, inclusive do Brasil, o qual teve que se adequar a nova realidade que estava enfrentando. As medidas de

[5] A COVID-19 é uma doença infecciosa causada pelo vírus SARS-CoV-2.

prevenção da doença advertiam sobre o uso de máscaras, álcool em gel e principalmente o distanciamento social.

Para o cumprimento do distanciamento social, algumas saídas foram adotadas pelos estados da Federação, uma delas foi o ensino de forma remota, para dar continuidade no ano letivo, em meio às restrições impostas pelo coronavírus ás aulas presenciais foram suspensas e os alunos passaram a exercer as atividades de ensino de casa, por meio de recursos tecnológicos.

O *home office* modalidade de trabalho remoto, à distância, foi adotado por empresas públicas e privadas com o intuito de conter a propagação da doença, mais uma vez, a internet conquista espaço, já que os trabalhadores utilizaram tecnologia para exercer suas atividades laborais.

Os aplicativos de comunicação foram essenciais para muitos, pois mantiveram as pessoas próximas, já que não era recomendável fazer visitas a amigos e familiares. A tecnologia contribui inclusive com a saúde nos tempos de pandemia, o médico psiquiatra e psicogeriatra, João Paulo Branco, em entrevista ao Poder 360 disse:

> A tecnologia com certeza nos ajudou muito. Se não fosse pela tecnologia, a nossa situação seria muito pior, tanto na depressão quanto no isolamento psíquico. O carinho pode ser transmitido por mensagens, ligações e videochamadas, mesmo que não com a mesma plenitude [6].

Vale ressaltar, que a tecnologia e a internet são duas paralelas, já que nos casos supracitados é necessário ter o acesso à rede para acessar as salas de aula, ferramentas de trabalho e aplicativos de mensagens.

O avanço tecnológico provoca aumento dos crimes praticados no espaço virtual, os chamados crimes cibernéticos. Em depoimento ao Portal R7, a advogada Elaine Saad Castello Branco, pós-graduada em Direito das Relações Sociais pela PUC-SP, afirma, "novas modalidades de crimes utilizam os meios digitais no mesmo ritmo que avançam as novas tecnologias, desafiando os conceitos de formas de atuação típicas previstos nas leis vigentes” [7].

Conforme informações extraídas do site de notícias G1:

---

[6] SOARES, Gabriella; BUSS, Gabriel. Em 1 ano de pandemia, tecnologia se torna central para a vida do brasileiro. Poder 360, 2021. Disponível em: https://www.poder360.com.br/coronavirus/em-1-ano-de-pandemia-tecnologia-se-torna-central-para-a-vida-do-brasileiro/. Acesso em: 25\10\2021.

[7] GOUSSINSKY, Eugenio. Crimes digitais têm forte alta em vários estados; saiba como prevenir. Portal R7, 2021. Disponível em: https://noticias.r7.com/tecnologia-e-ciencia/crimes-digitais-tem-forte-alta-em-varios-estados-saiba-como-prevenir-05052021. Acesso em: 25/10/2021.

> O número de denúncias anônimas de crimes cometidos pela internet mais que dobrou em 2020. De janeiro a dezembro do ano passado, foram 156.692 denúncias anônimas, contra 75.428 em 2019. Os dados levam em conta as notificações recebidas pela Central Nacional de Denúncias de Crimes Cibernéticos, uma parceria, da ONG Safernet Brasil com o Ministério Público Federal (MPF). O total de 156.692 é o maior número da série histórica desde que o levantamento começou, em 2014 [8].

As denúncias em relação a delitos praticados na internet aumentaram durante a pandemia. O estelionato virtual é um desses crimes cometidos na rede, do qual diversos estados brasileiros registraram alta nas ocorrências deste fato, dentre eles o Mato Grosso do Sul.

Conforme dados da Secretária de Estado de Justiça e Segurança Pública (SEJUSP) do Mato Grosso do Sul, os golpes virtuais tiveram um aumento de 49,28% durante a pandemia, ainda, segundo a secretária, pode se atribuir essa elevação como consequência do uso intenso da internet nesse período [9].

O famoso golpe do Whatsapp representa grande parte dessas ocorrências. Para realizar a ação os criminosos clonam o aplicativo e enviam mensagens para os contatos e lhes pede dinheiro se passando pela vítima. Há também diversos casos em que os criminosos fingem que a vítima trocou de telefone e com outro número de celular entram em contato e pedem dinheiro [10].

Em 2020, em comparação com o ano anterior, a Secretária de Segurança Pública do Estado do Rio Grande do Sul constatou que o crime de estelionato cresceu 25% durante o isolamento social [11].

No Amazonas o aumento foi de 216%, segundo relação feita pela Delegacia Interativa (DI), da Polícia Civil do Amazonas, de janeiro a maio de 2020, foram registradas 133 denúncias de estelionatos praticados no âmbito virtual, enquanto no mesmo período do ano anterior, foram registradas apenas 42 ocorrências [12].

---

8 Denúncias de crimes cometidos pela internet mais que dobram em 2020. G1. 09/02/2021. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/02/09/numero-de-denuncias-de-crimes-cometidos-pela-internet-mais-que-dobra-em-2020.ghtml. Acesso em: 25/10/2021.

9 MOREIRA, Rafaela. Golpes virtuais aumentam quase 50% em MS na pandemia; saiba como se proteger. Correio do Estado, 2021. Disponível em: https://correiodoestado.com.br/cidades/golpes-virtuais-aumentam-quase-50-em-ms-na-pandemia/385464. Acesso em: 25/10/2021.

10 Idem.

11 GRIZOTTI, Giovani. Golpes e crimes virtuais aumentam durante a pandemia no RS. G1, 2020. Disponível em: https://g1.globo.com/rs/rio-grande-do-sul/noticia/2020/06/15/golpes-e-crimes-virtuais-aumentam-durante-a-pandemia-no-rs.ghtml. Acesso em: 25/10/2021.

12 Delegacia Interativa registra aumento de mais de 200% em crimes de estelionato por meio da internet. Governo do Estado do Amazonas. Disponível em:

Ainda, segundo Delegacia Interativa do Amazonas, em abril e maio de 2020, período em que as medidas de isolamento social ficaram rígidas por conta da pandemia, foram registradas 93 ocorrências, enquanto, nos mesmos meses em 2019, foram apenas 18 denúncias [13].

O Distrito Federal também sofreu com o aumento do crime de estelionato durante a pandemia, conforme a Policia Civil do Distrito Federal (PCDF) o aumento no registro de denúncias pelo fato aumentou 198% [14].

Estes dados demonstram o quanto prejudicial pode ser a tecnologia e a internet juntas, visto que, atualmente os criminosos virtuais não necessitam de especialização para cometerem crimes, e a vulnerabilidade dos dados contidos na rede é de enorme, devemos nos preocupar com essa geração de crimes cibernéticos que aumenta gradativamente.

http://www.amazonas.am.gov.br/2020/06/delegacia-interativa-registra-aumento-de-mais-de-200-em-crimes-de-estelionato-por-meio-da-internet/. Acesso em: 25/10/2021.

[13] Delegacia Interativa registra aumento de mais de 200% em crimes de estelionato por meio da internet. Governo do Estado do Amazonas. Disponível em: http://www.amazonas.am.gov.br/2020/06/delegacia-interativa-registra-aumento-de-mais-de-200-em-crimes-de-estelionato-por-meio-da-internet/. Acesso em: 25/10/2021.

[14] FONSECA, Jaqueline. Registros de golpes na internet crescem 310% no DF durante a pandemia. Correio Braziliense, 2020. Disponível em: https://www.correiobraziliense.com.br/cidades-df/2020/08/4868977-mais-golpes-na-pandemia.html. Acesso em: 25/10/2021.

2. O ESTELIONATO VIRTUAL NA LEGISLAÇÃO BRASILEIRA

Este capítulo tem a finalidade de dispor sobre o crime de estelionato virtual e sua previsão no ordenamento jurídico brasileiro. Inicialmente far-se-á uma breve apresentação da teoria do crime, para fins de compreensão da sanção penal imposta pelo Estado aos indivíduos que violam as normas penais.

Proximamente serão feitas observações a respeito do crime de estelionato comum, sua previsão no Código Penal, bem como sua conceituação e demais informações relevantes sobre o tema.

Por fim, sucederão disposições gerais acerca do crime de estelionato virtual, o qual conquistou tipificação no ordenamento jurídico com o advento da Lei nº 14.155\2021, além disso, serão tratadas das alterações e demais incorporações que essa nova lei trouxe tanto no Código Penal quanto no Código de Processo Penal.

2.1. DO CRIME

A sanção penal é uma punição imposta pelo Estado aos agentes que violam as normas jurídicas. Para compreendermos essa sanção é necessário saber o significado de crime, para isso, abordar-se à sua teoria. Guilherme de Souza Nucci (2021, p. 239), conceitua crime sob três aspectos, são eles: material, formal e analítico:

> Em suma, no sentido material, o crime é a conduta ofensiva a um bem juridicamente tutelado, ameaçada de pena [...] Na concepção formal, o crime é exatamente a conduta descrita em lei como tal. Para isso, utiliza-se o critério de existência de um tipo penal incriminador. Existindo, há o delito em tese [...] O conceito analítico cuida da concepção da ciência do direito, acerca do crime, visando apenas estudá-lo e, didaticamente, torná-lo bem compreensível ao operador do direito. Portanto, disseca-se o conteúdo do conceito formal de delito para dele extrair os seus elementos.

Toledo (1999, p. 30) leciona sobre o conceito analítico do crime:

> Substancialmente, o crime é um fato humano que lesa ou expõe a perigo bens jurídicos (jurídico-penais) protegidos. Essa definição é, porém, insuficiente para a dogmática penal, que necessita de outra mais analítica, apta a pôr à mostra os aspectos essenciais ou elementos estruturais do conceito de crime. E dentre as várias definições analíticas que tem sido propostas por importantes penalistas, parece-nos mais aceitável a que considera as três notas fundamentais do fato-crime, a saber: ação típica

> (tipicidade), ilícita ou antijurídica (ilicitude) e culpável (culpabilidade). O crime, nessa concepção que adotamos, é, pois, ação típica, ilícita e culpável.

Na mesma linha de conceituação de Nucci, seguem outros doutrinadores, como, Fernando Capez e Rogério Greco. Atualmente, o conceito de crime que predomina é o adotado pela abordagem analítica da teoria tripartida do crime, a qual dispõe que crime é um fato típico, ilícito e culpável e somente existe na presença desses três elementos (NUCCI, 2021).

2.2. O CRIME DE ESTELIONATO

A denominação estelionato deriva de *stellio,* proveniente do latim, quer dizer “lagarto que muda de cores, iludindo os insetos de que se alimenta” (MIRABETE, FABBRINI, 2021, p.322). Pode-se dizer que o lagarto a que se refere à definição acima, é o camaleão, visto que, este possui como uma das suas principais características a mudança de cor, com o intuito de se adaptar em qualquer ambiente, visando enganar seus predadores e facilitar na captura de alimentos.

Podemos comparar o réptil, com o estelionatário, sujeito ativo do presente delito, visto que, este também possui facilidade em se adaptar no meio social em que habita, agindo desonestamente, com disfarces e enganos com a finalidade de iludir as vítimas com suas conversas fraudulentas para alcançar seu objetivo final, que é obter alguma vantagem ilícita.

No Brasil, o crime de estelionato está descrito no artigo 171 do Decreto-Lei nº 2.484 de 07 de dezembro de 1940- o Código Penal Brasileiro, abaixo aduzido:

> Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:
> Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis [15].

O estelionato é um crime contra o patrimônio, no entanto, em segundo plano, o dispositivo protege também a boa-fé, segurança, fidelidade e veracidades dos negócios jurídicos patrimoniais (MIRABETE, FABBRINI, 2021). No que concerne aos sujeitos do delito, para Prado (2020) o sujeito ativo pode ser qualquer pessoa natural,

[15] BRASIL. Código Penal (1940), Capítulo VI- Do estelionato e outras fraudes, art. 171. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm. Acesso em: 15\11\2021.

pois se trata de crime comum, já o sujeito passivo, pode ser pessoa natural ou jurídica que sofra lesão patrimonial.

A conduta do estelionato é caracterizada com o emprego de artificio ardil ou qualquer outro meio fraudulento para obter vantagem ilícita. Segundo (MIRABETE, FABBRINI, 2021, p. 325):

> Artifício existe quando o agente se utilizar de um aparato que modifica, ao menos aparentemente, o aspecto material da coisa, figurando entre esses meios o documento falso ou outra falsificação qualquer, o disfarce, a modificação por aparelhos mecânicos ou elétricos, filmes, efeitos de luz etc. O ardil é a simples astúcia, sutileza, conversa enganosa, de aspecto meramente intelectual. Tem-se entendido, corretamente, que a simples mentira, se hábil a enganar, configura o ardil.

No que tange ao tipo penal referindo-se a qualquer outro meio fraudulento, sabe-se que este meio deve idôneo a enganar a vítima, segundo Mirabete e Frabbrini (2021, p. 325):

> Discute-se, na aferição da idoneidade do meio empregado, se deve ser levada em consideração a prudência ordinária, o discernimento do *homo medius*, ou a pessoa da vítima, concluindo os doutrinadores por esta última hipótese. Embora já se tenha decidido que as manobras fraudulentas devem ser suficientes para embair a média argúcia, a prudência normal, aquele mínimo de sagacidade que a pessoa comum usa em seus negócios, é francamente predominante a jurisprudência de que a idoneidade do meio deve ser pesquisada no caso concreto, inclusive tendo-se em vista as condições pessoais da vítima.

Exige-se do agente o elemento subjetivo, que é o dolo, ou seja, a vontade de obter ilicitamente vantagem patrimonial, tanto para si quanto para outrem. Vale ressaltar ainda, que no presente crime não é admitida a modalidade culposa (MIRABETE, FABBRINI, 2021).

A consumação do delito se dá “com a obtenção da vantagem ilícita, em prejuízo alheio, ou seja, com o dano, no momento em que a coisa passa da esfera de disponibilidade da vítima para aquela do infrator” (MIRABETE, FABBRINI, 2021, p. 328). Há também a possibilidade de tentativa, a qual se restará caracterizada quando o agente não obtendo vantagem, pudesse consegui-la.

Existe o crime, portanto, quando o autor utiliza qualquer meio fraudulento para induzir alguém em erro ou mantê-lo nessa situação, conseguindo assim, uma vantagem indevida para si ou para outrem, com lesão patrimonial alheia.

2.3. DO ESTELIONATO VIRTUAL

Assim como os demais ramos, o Direito Penal é redigido por uma série de princípios, sendo que um dos principais é o Princípio da Reserva legal, o qual está preconizado no art. 1º do Código Penal Brasileiro: “não há crime sem lei anterior que o defina. não há pena sem prévia cominação legal” [16]. Diante disso, somente serão puníveis os atos que estiverem previstos em lei como ilícitos, sendo que a Lei Penal deve ser interpreta de forma restrita, não podendo fazer analogia para abarcar situações semelhantes não descritas na legislação.

Justamente dai surgia o impasse, quando o ordenamento jurídico brasileiro se mostrava inerte quanto à tipificação do estelionato virtual. A insuficiência de normas que abrangessem os crimes virtuais tornava-se um problema social que atingia a população no geral. A própria Constituição Federal de 1988 traz no inciso XXXIX do art. 5º o princípio da legalidade, o qual também se encontra descrito no Código Penal:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> [...]
> XXXIX - não há crime sem lei anterior que o defina, nem pena sem prévia cominação legal [17].

Com base no mencionado princípio, conclui-se que qualquer indivíduo que cometa algum crime deve ser punido de acordo com a conduta tipificada como ilícita pela legislação, ou seja, o ato deve se enquadrar perfeitamente na letra da Lei, não podendo ser reprovável sem que cumpra os requisitos de validade.

2.3.1. Do advento da Lei nº 14.155\2021

Com o advento da Lei nº 14.155\2021 os crimes virtuais tornaram-se mais abrangentes, diminuindo os impactos causados na sociedade pela falta de tipificação

---

[16] BRASIL. Código Penal (1940), Título I- Parte Geral, Da aplicação da Lei Penal, art. 1º. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm. Acesso em: 15\11\2021.
[17] BRASIL. Constituição Federal (1988). Título II- Dos Direitos e Garantias Fundamentais. Capítulo I- Dos Direitos e Deveres individuais e coletivos, art. 5º, XXXIX. Disponível em: https://www.planalto.gov.br/ccivil_03/Constituicao/ConstituicaoCompilado.htm. Acesso em: 15\11\2021.

no ordenamento jurídico. Com a chegada dessa lei o estelionato virtual foi descrito no Código Penal.

O Projeto de Lei nº 4.554\2020 de autoria do Senador Izalci Lucas (PSDB\DF), após sanção do Presidente Jair Bolsonaro, foi convertido em Lei no dia 27 de maio de 2021. A Lei nº 14.155\2021 tem como um dos seus principais objetivos qualificar ilícitos praticados mediante fraudes eletrônicas, tornando mais gravosas as penas aplicáveis, sendo assim, trouxe alterações ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) e ao Decreto-Lei nº 3.689 de 3 de outubro de 1941 (Código de Processo Penal), os quais necessitavam destes ajustes, levando em conta a realidade atual [18].

A Lei nº 12.737\2012 apelidada de “Lei Carolina Dieckmann” em razão da atriz brasileira que teve seu dispositivo informático invadido, sofreu alterações em seu texto legal, e ainda, os crimes de furto e estelionato também sofreram modificações [19]. A seguir será apresentado um quadro comparativo com a redação anterior e a atual inserida no art. 154-A do Código Penal, que versa sobre a invasão de dispositivo informático:

- Tabela 2- Comparativo da redação anterior com a redação atual do art. 154-A do Código Penal

Redação anterior	Redação atual
Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.	Art. 154-A. Invadir dispositivo informático **de uso** alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do **usuário** do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita.
Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.	Pena - **reclusão, de 1 (um) a 4 (quatro) anos, e multa**.
§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.	§ 2º Aumenta-se a pena de **1/3 (um terço) a 2/3 (dois terços)** se da invasão resulta prejuízo econômico.

[18] PINHEIRO, Patricia Peck. FILHO, Genival Silva Souza. SHINOHARA, Luciane. AVANÇO, Rafaella. A nova lei de combate as fraudes eletrônicas. Migalhas. Disponível em: https://www.migalhas.com.br/depeso/347511/a-nova-lei-de-combate-as-fraudes-eletronicas. Acesso em: 15\11\2021.
[19] Idem.

Fonte: Art. 154-A do Código Penal.

Como se pode observar no quadro o mencionado artigo sofreu algumas alterações em seu texto em relação ao uso do dispositivo, não sendo necessário que a vítima seja proprietária do dispositivo informático, podendo ser meramente usuária. Outra modificação ocorreu em relação a pena do delito que se tornou o mais gravosa.

Diferente do descrito acima, o art. 155 do Código Penal, recebeu um novo parágrafo, o qual aduz sobre o furto praticado mediante fraude por meio de dispositivo eletrônico ou informático, conectado ou não a rede, observe:

- Tabela 3- Redação do parágrafo 4º incorporado ao art. 155 do Código Penal

Art. 155 [...]	Art. 155 (...) § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo. § 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso: I - aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional; II - aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável.

Fonte: Art. 155§4º do Código Penal

Uma atenção especial deve ser dada ao novo parágrafo inserido no art. 171 do Código Penal, pois se trata do crime em questão e, além disso, foi ele quem resolveu o impasse da falta de tipificação do estelionato virtual no ordenamento jurídico brasileiro:

- Tabela 4- Redação dos parágrafos 2º-A e 2º-B incorporados ao art. 171 do Código Penal

	Art. 171 (...) Fraude eletrônica § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes

Art. 171 [...]	sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo. § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional.

Fonte: Art. 171§2ª-A §2º-B

A nova lei dedica-se a agravar os crimes cometidos de forma eletrônica ou pela internet. Atualmente os crimes cibernéticos atingiram grandes proporções em razão da evolução tecnológica e conforme já afirmado anteriormente, a pandemia da COVID-19, contribui ainda mais com esse crescimento, visto que, a população começou a se familiarizar com as ferramentas digitais, para realizarem atividades de rotina, como comprar e vender, pagar e receber. Em razão disso, o momento traz consigo a necessidade de uma legislação que busca garantir a segurança da informática e da cibernética, diminuindo os impactos negativos causados pelas fraudes.

Nota-se que com o advento da presente lei, se atingiu maior abrangência de crimes virtuais no Código Penal, o que contribui com a diminuição da deficiência normativa a respeito destes respectivos crimes. Há que se falar também que a nova Lei incorporou ao Código de Processo Penal Brasileiro um parágrafo dedicado à competência para processar crimes de estelionato, o qual será aprofundado em outro tópico [20].

2.3.2. Disposições gerais relativas ao estelionato virtual

Para que haja a consumação do delito de estelionato é necessário que o autor utilize qualquer meio fraudulento para induzir alguém a erro ou mantê-lo nessa situação, conseguindo assim, uma vantagem indevida para si ou para outrem, com lesão patrimonial alheia (MIRABETE, FABBRINI, 2021). O estelionato virtual se difere do estelionato comum apenas em relação ao meio de execução, já que para que se

[20] PINHEIRO, Patricia Peck. FILHO, Genival Silva Souza. SHINOHARA, Luciane. AVANÇO, Rafaella. A nova lei de combate as fraudes eletrônicas. Migalhas. Disponível em: https://www.migalhas.com.br/depeso/347511/a-nova-lei-de-combate-as-fraudes-eletronicas. Acesso em: 15\11\2021.

consume o primeiro, é necessário que o agente utilize um dispositivo tecnológico conectado ou não a rede de internet.

Quando se fala em crimes virtuais logo vêm na mente que os autores destes são pessoas especializadas, como os hackers ou crackers. No entanto, se trata de crime comum, e pode ser praticado por qualquer pessoa que possua conhecimentos mínimos sobre dispositivos eletrônicos. No que diz respeito à vítima, está pode ser tanto pessoa física quanto pessoa jurídica.

Uma das principais formas de cometimento do delito em tela é através do *e-commerce* (comércio eletrônico), no qual diversas pessoas são vítimas destes estelionatários, que desenvolvem sites de vendas apenas com a finalidade de fraudar, ou seja, a vítima efetua a compra e faz o pagamento, porém não recebe o produto adquirido (WENDT, JORGE, 2012).

A prática desse tipo de crime também é repetidamente ocasionada através do envio de e-mails, onde supostamente a vítima recebe um correio eletrônico de uma renomada instituição financeira que solicita a confirmação e atualização de dados cadastrais, assim, o estelionatário se passa por um banco para solicitar tais dados e posteriormente usá-los para obtenção de vantagem indevida (WENDT, JORGE, 2012).

Nota-se que os estes criminosos virtuais utilizam-se de técnicas para enganar as vítimas e incentiva-las a conceder os dados que necessitam para obter determinada vantagem, ou então, a executar transferência de determinada quantia em dinheiro. Muitos artifícios são utilizados pelos sujeitos ativos do delito, estes métodos de ataque são chamados de engenharia social, que Segundo Wendt e Jorge (2012, p. 21) caracterizam-se pelo:

> [...] uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações. Exemplo: você recebe uma mensagem de e-mail, cujo remetente é o gerente ou alguém em nome do departamento de suporte do seu banco. Na mensagem ele diz que o serviço de Internet Banking está apresentando algum problema e que tal problema pode ser corrigido se você executar o aplicativo que está anexado à mensagem. A execução deste aplicativo apresenta uma tela análoga àquela que você utiliza para ter acesso à conta bancária, aguardando que você digite sua senha. Na verdade, este aplicativo está preparado para furtar sua senha de acesso à conta bancária e enviá-la para o atacante.

Um dos fatores que impressiona na prática deste delito é a criatividade dos criminosos e a capacidade em enganar a vítima e induzi-la a fazer o que ele deseja.

O estelionato virtual não possui uma prática definida, varia de acordo com o delinquente, os quais geralmente baseiam-se na manipulação de emoções como a ganância e curiosidade para despertar o interesse da vítima e consequente obter o que almeja. (WENDT, JORGE, 2012).

O mundo virtual oferece muitas vantagens aos seus usuários, entretanto, esse uso em massa da internet despertou o interesse dos estelionatários, que enxergam o âmbito virtual como um local oportuno para enganar as pessoas, justamente pela dificuldade de serem descobertos e consequentemente serem punidos.

2.3.3. Da competência para apuração do crime

Apresentadas as condições em que o estelionato virtual pode ser cometido, é necessário que haja uma definição do juízo competente para apreciar tais casos, já que, nem sempre quem sofre o prejuízo e quem obtém a vantagem encontra-se no mesmo local, tal situação gera dificuldades em se estabelecer com precisão onde o estelionatário alcançou seu proveito ilícito [21].

Como se sabe, no Processo Penal, em regra, a competência é fixada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução (art. 70 do Código de Processo Penal) [22].

Com o advento da Lei nº 14.155\2021, foi acrescentado ao art. 70 do Código de Processo Penal, um novo parágrafo, o qual dispõe sobre a competência quando os crimes de estelionato forem praticados mediante depósito ou emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado, ou mediante transferência de valores, aduz o §4º do referido art.:

> Nos crimes previstos no art. 171 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), quando praticados mediante depósito, mediante emissão de cheques sem suficiente provisão de fundos em poder do sacado ou com o pagamento frustrado ou mediante transferência de valores, a

[21] MOREIRA, Rômulo de Andrade. A nova competência criminal para o crime de estelionato e a questão dos processos pendentes. Empório do Direito. Disponível em: https://emporiododireito.com.br/leitura/a-nova-competencia-criminal-para-o-crime-de-estelionato-e-a-questao-dos-processos-pendentes. Acesso em: 15\11\2021.

[22] BRASIL. Código de Processo Penal (1941). Capítulo I- Da competência pelo lugar da infração. Art. 70. Disponível em: https://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del3689Compilado.htm. Acesso em: 15\11\2021.

> competência será definida pelo local do domicílio da vítima, e, em caso de pluralidade de vítimas, a competência firmar-se-á pela prevenção [23].

Antes da nova lei, havia uma divergência nos tribunais, justamente porque para se verificar a competência era preciso analisar a consumação do delito. No entanto, a consumação do delito varia, dependendo da forma como é praticado. Atualmente, essa divergência caiu por terra. Assim, de acordo com o princípio do Juiz Natural, apenas os casos de estelionato posteriores à nova lei terão a competência regida pelo local de domicílio da vítima [24].

[23] BRASIL. Código de Processo Penal (1941). Capítulo I- Da competência pelo lugar da infração. Art. 70§4º. Disponível em: https://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del3689Compilado.htm. Acesso em: 15\11\2021.

[24] GUEIROS, Guilherme. NUNES, Eliane. Lei dos “crimes cibernéticos” altera competência em caso de estelionato. Conjur. Disponível em: file:///D:/Users/SEVEN/Downloads/ConJur%20-%20Opini%C3%A3o_%20Lei%20dos%20'crimes%20cibern%C3%A9ticos'%20e%20compet%C3%AAncia%20no%20estelionato.pdf. Acesso em: 18\11\2021.

3. DAS DIFICULDADES NA APLICABILIDADE DA LEGISLAÇÃO

O presente capítulo será destinado a explicar as dificuldades na aplicabilidade da legislação. Neste tópico serão abordados assuntos como o lugar do crime, no que diz respeito aos crimes cibernéticos praticados em território estrangeiro, porém com resultado em território brasileiro, além disso, tratar-se-á de aspectos referentes à complexidade em se estabelecer de fato quem é o autor do crime cibernético e os obstáculos enfrentados na fase das investigações, bem como a necessidade de reunião de conjunto probatório e a possível necessidade perícia especializada.

3.1. DO LUGAR DO CRIME

Quando se trata de crimes cibernéticos, o lugar do crime é uma questão que necessita ser enfatizada, já que é possível que as condutas sejam praticadas em ambientes objetivamente muito distantes em relação ao resultado delituoso gerado (FILHO, 2021).

No que concerne à territorialidade no contexto das inovações digitais, leciona Pinheiro (2016, p. 84-86):

> No mundo tradicional, a questão da demarcação do território sempre foi definida por dois aspetos: os recursos físicos que esse território contém e o raio de abrangência de determinada cultura. A sociedade digital rompe essas duas barreiras: o mundo virtual constrói um novo território, dificilmente demarcável, no qual a própria riqueza assume um caráter diferente, baseada na informação, que, como vimos, é inesgotável e que pode ser duplicada infinitamente. (...) Para a sociedade digital, não é mais um acidente geográfico, como um rio, montanha ou baía, que determina a atuação do Estado sobre seus Indivíduos e a responsabilidade pelas consequências dos atos destes. A convergência, seja por Internet, seja por outro meio, elimina a barreira geográfica e cria um ambiente de relacionamento virtual paralelo no qual todos estão sujeitos aos mesmos efeitos, ações e reações.

O Código Penal Brasileiro adotou a teoria mista ou da ubiquidade, que segundo Nucci (2021, p. 183) dispõe que “é lugar do crime tanto onde houve a conduta quanto o local onde se deu o resultado”. Nesse sentido, alude o art. 5º do Código Penal: “aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional” [25]. No mesmo cerne do assunto

[25] BRASIL. Código Penal (1940). Parte Geral- Título I- Da aplicação da Lei Penal. Art. 5º. Disponível em: http://www.planalto.gov.br/ccivil_03/Decreto-lei/Del2848compilado.htm. Acesso em: 20\11\2021.

dispõe o art. 6º do mesmo diploma: “considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado” [26].

Ante a exposição dos artigos mencionados acima, nota-se que não importa o caminho que o sujeito ativo do crime cibernético percorra, aplicar-se-ão as disposições penais brasileiras quando aqui for realizada a conduta ou aqui se produzir o resultou ou dever produzi-lo. Nesse sentido, observe:

> Para a aplicação da Lei Penal, o Estado brasileiro titular do jus puniendi adotou, como regra, o princípio da territorialidade, conforme já citado art. 5º do Código Penal, sem prejuízo da incidência de outros princípios nos casos dispostos no art. 7º, inciso II, do mesmo diploma legal. E, para a definição do lugar do delito, optou o legislador penal pela adoção do Princípio da Ubiquidade (art. 6º do CP), estabelecendo que se considera praticado o crime “no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde produziu ou devera produzir-se o resultado”. Da análise dos artigos acima mencionados, infere-se que, na prática de crimes por meio da internet, ocorrida no território nacional, torna-se completamente irrelevante para a aplicação da lei penal o local em que fica a sede da empresa provedora do serviço de internet ou onde estão armazenadas as informações telemáticas. Portanto, se um crime cibernético ocorreu no Brasil, estará sujeito à jurisdição brasileira, sendo dever do Estado investigar e reprimir as condutas delituosas praticadas e fazer cumprir as decisões emanadas de juiz brasileiro para a efetiva apuração do delito, sem a necessidade de cooperação internacional para o cumprimento da decisão [27].

Como observado o lugar do crime não se reveste de dificuldade para o ordenamento jurídico brasileiro para fins de aplicação da Lei Penal. No entanto, este realmente não é o cerne da questão, foi explanado a respeito somente para fins de compreensão do tema. A descoberta da autoria é o verdadeiro problema a ser enfrentado e tal será o assunto seguinte.

3.2. DA AUTORIA

Para que a sanção penal seja imposta ao sujeito, é necessário que este tenha praticado a conduta caracterizada como crime cibernético (RAMOS, 2017). A principal preocupação com relação aos crimes cibernéticos é justamente no que diz respeito à autoria destes. A correta identificação do criminoso é indispensável para que a

---

[26] BRASIL. Código Penal (1940). Parte Geral- Título I- Da aplicação da Lei Penal. Art. 6º. Disponível em: http://www.planalto.gov.br/ccivil_03/Decreto-lei/Del2848compilado.htm. Acesso em: 20\11\2021.
[27] BRASIL. MINISTÉRIO PÚBLICO FEDERAL. Crimes cibernéticos: coletânea de artigos, Brasília, MPF, 2018, 3ª ed., p. 36.

pretensão punitiva seja justa e direcionada aquele que realmente violou aos preceitos jurídicos preconizados na legislação.

A principal característica do crime informático é a ausência física do criminoso. Conforme Guilherme Schmitt (2014) o agente que comete delitos no âmbito virtual raramente utiliza de sua real identificação pessoal, diversas vezes se passa por terceiros. Há também, diversos casos em que o individuo através de estratégias computacionais se utiliza de perfis anônimos para infringir as normas e se manter impune (AZEVEDO, CARDOSO, 2021).

No entanto, da mesma forma com que pessoas possuem números como identificação, como o CPF e o RG, os computadores e demais eletrônicos conectados á internet também são identificados através de um número, o IP *(Internet Protocol)* (AZEVEDO, CARDOSO, 2021). De modo semelhante relata Ramos (2017, p.53):

> No “mundo real”, a identificação de uma pessoa na sociedade mescla uma espécie de concretização qualitativa, que corresponde a uma identificação visual, através do reconhecimento das principais características do indivíduo tais como feições, altura, voz; com uma espécie de concretização numérica, que corresponde a um reconhecimento e identificação legal, através do número de um documento como o passaporte ou registro geral. No mundo virtual, a identificação do endereço IP corresponde à concretização numérica, contudo, a grande diferença é que esse número identifica o computador e não uma pessoa.

A princípio o anonimato é apenas aparente, já que através do número de IP é possível chegar á maquina que foi utilizado como instrumento para cometer o delito. Nesse sentido, alude Filho (2021, p. 267):

> Assim, quando se busca identificar um sujeito no contexto da Internet, deve-se partir do endereço da máquina: nas redes de computadores, não é possível identificar o usuário visualmente ou através de documentos, mas é possível identificar o endereço da máquina que envia as informações à rede. Ou seja, o IP da máquina. Este é uma identificação única para cada computador ligado à rede. Nos termos da Lei 12.965/14, endereço de protocolo de internet (endereço IP) é o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais (art. 5º, III).

Há outra forma de se obter informações acerca do acesso á rede, e é através do servidor proxy, o qual, segundo Ramos (2017, p. 54) é: “responsável por armazenar os logs de registro de navegação que identificam os locais acessados pelo usuário, bem como os serviços utilizados, quando a conexão com a rede mundial de computadores é direta”.

A investigação criminal deve considerar todo e qualquer rastro deixado pelo criminoso cibernético e usá-lo para descobrir a autoria. No entanto, isso somente será possível se a conexão for direta. Apesar da existência dessas duas espécies de identificação de conexão, é possível faze-la de forma indireta a qual não é passível de rastreamento (RAMOS, 2017).

A identificação do autor e sua qualificação são requisitos essenciais para a instrução processual penal. A investigação dos crimes cibernéticos é realizada por etapas, e a primeira delas é a identificação da origem da comunicação. Através de uma análise trafego de dados se chegará ao endereço IP de origem. Após isso, serão colhidas possíveis provas da prática do delito. Há que mencionar que decorrido todo esse processo, o qual é extremamente complexo, se chegará à identificação da maquina, e não do real autor, visto que, o criminoso pode utilizar um computador de um local público, como uma biblioteca ou cybercafé para cometimento do delito. Justamente dai surge o problema (RAMOS, 2017).

A dificuldade decorrente da identificação de autoria está em relacionar o computador e o sujeito que opera em determinado espaço de tempo. A identificação do criminoso cibernético, conforme Ramos (2017), de maneira inequívoca, é possível somente através das impressões digitais ou do reconhecimento facial.

A identidade digital obrigatória pode ser considerada um dos temas mais importantes para o Direito atualmente, conforme Pinheiro (2013) a “ausência de uma lei para gerar prova de autoria e de um entendimento consolidado e unificado incorre em várias possibilidades de entendimento por parte do juiz quando se depara com um crime cibernético”.

Vale mencionar que, a investigação de um crime cibernético encontra dois obstáculos: o primeiro é correlacionar o endereço IP identificado com a máquina utilizada para a prática do delito e o segundo é de que maneira relacionar a máquina com o sujeito que a opera (RAMOS, 2017).

3.3. DA OBTENÇÃO DE PROVAS

O termo prova origina-se do latim *probatio* que significa: ensaio, verificação, inspeção, exame, argumento, razão, aprovação ou confirmação. Nucci (2021, p. 260) dispõe: “a meta da parte, no processo, portanto, é convencer o magistrado, por meio

do raciocínio, de que a sua noção da realidade é a correta, isto é, de que os fatos se deram no plano real exatamente como está descrito em sua petição".

A reconstrução da verdade é o principal objetivo da prova judiciária. É neste momento em que se busca a existência entre os fatos investigados e a verdade real. É o material probatório colhido durante as investigações que irá compreender a autoria e materialidade do delito e posteriormente irá gerar o convencimento do magistrado a respeito dos fatos objetos da lide. (RAMOS, 2017).

Os meios de provas podem ser lícitos ou ilícitos, no entanto, somente os primeiros são levados em consideração pelo juiz, visto que, os segundos são contrários ao ordenamento jurídico. Vale ressaltar que todas as provas são admitidas desde que não contrariem as normas jurídicas (NUCCI, 2021).

Nesse sentido, são validas as provas eletrônicas das quais versam o art. 225 do Código Civil Brasileiro:

> 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 [28].

O juiz dispõe de livre convencimento motivado e poderá apreciar livremente as provas (NUCCI, 2021).

No que concerne à coleta inicial de provas, o instrumento utilizado para apurar a prática de um crime e sua autoria é o inquérito policial, e é através dele que serão colhidos os indícios do crime cometido no âmbito virtual. "O inquérito policial é um procedimento preparatório da ação penal, de caráter administrativo, conduzido pela polícia judiciária e voltado à colheita preliminar de provas para apurar a prática de uma infração penal e sua autoria" (NUCCI, 2021, p.73).

A polícia investigativa encontra muitas dificuldades na apuração de crimes cibernéticos, já que, os criminosos comumente utilizam-se de experiências com o computador para desenvolver estratégias com o intuito de não ser descoberto. Vale elucidar que soluções estão sendo procuradas, como por exemplo, uma melhor capacitação dos agentes responsáveis pela persuasão penal (AZEVEDO, CARDOSO, 2021).

---

[28] BRASIL. Código Civil (2002). Título V- Da prova. Art. 225. Disponível em: https://corpus927.enfam.jus.br/legislacao/cc-02. Acesso em: 20\11\2021.

O inquérito policial é um procedimento administrativo cautelar, e além da coleta de provas documentais, testemunhais ou periciais, poderá trazer atos de instrução não provisória, como buscas e apreensões (NUCCI, 2021). No que diz respeito às funções do respectivo procedimento, menciona Ramos (2017, p. 57).

> Renato Brasileiro de Lima atribui duas funções ao inquérito policial: uma função preservadora e uma função preparatória. Enquanto a primeira evita a instauração de um processo infundado; a segunda fornece elementos ao titular da ação penal, para que este ingresse em juízo, além de resguardar meios de prova que poderiam se perder no decorrer do processo.

Ante a função preservadora, o inquérito policial, poderá produzir as provas cautelares, não repetíveis e antecipadas, as quais podem perecer com o decorrer do tempo. No entanto, terá validade somente se considerada indispensável para pronuncia da sentença e houver indícios suficientes que a respectiva prova realmente estava sob risco de perecimento.

Cabe salientar a importância da investigação no âmbito virtual, visto que, inocentes podem ser culpados por terem suas contas invadidas ou clonadas, as quais são utilizadas por terceiro para o cometimento de atos ilícitos, sendo assim, a pretensão punitiva deve incorrer sobre quem realmente praticou o crime (AZEVEDO, CARDOSO, 2021).

3.4. DA NECESSIDADE DE PERICIA ESPECIALIZADA

A computação forense é a ferramenta utilizada na investigação e coleta de evidências dos atos ilícitos praticados por meio de computadores conectados á rede de internet, pode ser considerada como a ciência dedicada a explicar os fatos por meio da utilização de métodos científicos na coleta, validação e identificação das evidencias digitais para que se possam punir os criminosos. Esse mecanismo surgiu em decorrência do crescimento da utilização dos aparelhos eletrônicos e da internet para pratica de crimes (RAMOS, 2017).

As evidências dos crimes cibernéticos poderão ser retiradas de quaisquer dispositivos eletrônicos, sejam eles, computadores, celulares ou discos rígidos. As evidências digitais, conforme Pinheiro (2013, p. 216) podem ser definidas como: “toda informação retirada de um compilado ou depositário eletrônico, através da intervenção humana ou não, em um formato inteligível ao ser humano”.

As provas eletrônicas extraídas das investigações dos crimes cibernéticos necessitam passar por pericias especializadas em decorrência da vulnerabilidade dos dados, os quais possuem facilidade em serem adulterados. Essa perícia ira garantir a validade e integridade dos resultados (RAMOS, 2017).

São exemplos de indícios que podem ajudar nas investigações dos crimes cibernéticos: arquivos de imagem, mensagens eletrônicas, arquivos com informações ou dados roubados (PINHEIRO, 2013).

Os crimes cibernéticos são considerados complexos, uma vez que se desenvolvem e se consumam em um ambiente virtual, e conforme já disposto anteriormente não há a presença física do sujeito ativo. Ainda, contribui com essa complexidade a facilidade do perecimento das provas às quais podem sofrer alterações, serem perdidas ou até mesmo apagadas, como é o caso de fotografias, vídeos, imagens ou arquivos digitais. (RAMOS, 2017).

Em decorrência da vulnerabilidade das provas eletrônicas, exige-se um perito especializado para proceder a sua análise, visto que, se feita erroneamente estará violando princípios constitucionais e disposições do direito material, podendo tornar-se ilícita ou inválida.

Diante dessa minuciosidade exigida nas perícias, um dos maiores problemas em relação à produção de provas nos crime cibernéticos é justamente o despreparo da polícia investigativa e da perícia. Os profissionais capacitados para esse tipo de investigação são poucos e é indispensável que se atenda as exigências técnicas para evitar que decorram questionamentos sobre a identidade da prova e a licitude de sua obtenção (RAMOS, 2017).

> Com o intuito de dar legitimidade às provas produzidas nos crimes virtuais, a investigação criminal e a instrução processual demandam procedimentos técnicos. Os profissionais especializados em hardware, software, tráfego e segurança de rede, através da realização de exames periciais, buscarão apontar a veracidade dos fatos. A eficiência da investigação criminal será resultado da atuação desses peritos na análise do ambiente aonde o crime foi praticado e na constatação da veracidade (RAMOS, 2017, p. 50).

Diversos Estados como São Paulo, Rio de Janeiro, Espirito Santo, Minas Gerais, Paraná, Rio Grande do Sul, Distrito Federal, Goiás, Pará, Mato Grosso e

Sergipe contam com delegacias especializadas na repressão de crimes cibernéticos[29].

Observa-se que o país esta se preparando para combater os crimes cibernéticos, com a criação de delegacias especializadas e através da capacitação dos profissionais responsáveis por investigar tais crimes, no entanto, a quantidade, tanto de delegacias quanto de profissionais não é suficiente para apurar o referido delito, uma vez que os crimes cibernéticos tiveram alta em decorrência das evoluções tecnológicas.

[29] MOZART, Santos Pedro. Denunciar crimes virtuais: lista de delegacias especializadas. Disponível em: http://santospedro.com.br/quero-denunciar-crimes-virtuais-lista-de-delegacias-especializadas/. Acesso em: 20\11\2021.

4. CONVENÇÃO SOBRE CRIME CIBERNÉTICO

A Convenção sobre Crime Cibernético, conhecida também como Convenção de Budapeste foi desenvolvida por países da União Europeia e está em vigor desde 2004. È o primeiro tratado internacional a dispor sobre crimes virtuais, tal possui como objetivo proteger a sociedade dos criminosos do ciberespaço, adotando para isso, uma legislação adequada e melhorando a cooperação internacional [30].

O preâmbulo da convenção dispõe:

> "[...] a presente Convenção é necessária para impedir os actos praticados contra a confidencialidade, integridade e disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta de desses sistemas, redes e dados, assegurando a incriminação desses comportamentos tal como descritos na presente Convenção, e da adopção de poderes suficientes para combater eficazmente essas infracções, facilitando a detecção, a investigação e o procedimento criminal relativamente às referidas infracções, tanto ao nível nacional como internacional, e estabelecendo disposições materiais com vista a uma cooperação internacional rápida e fiável" [31].

Nos 48 artigos do tratado são definidas as medidas que devem ser adotadas pelos países signatários no combate aos crimes cibernéticos, como a elaboração de legislação penal e processual para estes tipos de delitos [32].

Em 2019, o governo brasileiro recebeu um convite com validade de três anos para aderir o tratado. O Projeto de Decreto Legislativo (PDL) 255\2021 aprovou o texto da Convenção. No dia 06 de outubro de 2021 a Câmara dos Deputados aprovou o projeto de adesão do Brasil à Convenção, no entanto, para se incorporar a legislação brasileira, será necessário passar por apreciação do Senado Federal.[33]

O Senado Federal irá apreciar a referida Convenção e votar pela incorporação ou não da mesma as normas do país, se aprovada, o Brasil terá acesso a mecanismos

---

[30] Câmara aprova adesão brasileira a tratado internacional de cibercrimes. Disponível em: https://canaltech.com.br/seguranca/camara-aprova-adesao-brasileira-a-tratado-internacional-de-cibercrimes-198233/. Acesso em: 20\11\2021.

[31] Convenção sobre cibercrime. Disponível em: http://mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf. Acesso em: 20\11\2021.

[32] JUNIOR, Janary. Projeto aprova adesão do Brasil á convenção europeia sobre crime cibernético. Disponível em: https://www.camara.leg.br/noticias/779447-projeto-aprova-adesao-do-brasil-a-convencao-europeia-sobre-crime-cibernetico/. Acesso em: 20\11\2021.

[33] Idem.

que facilitaram as investigações dos crimes virtuais, já que contará com a cooperação das autoridades policiais, judiciais e órgãos de investigações internacionais [34].

[34] Câmara aprova adesão brasileira a tratado internacional de cibercrimes. Disponível em: https://canaltech.com.br/seguranca/camara-aprova-adesao-brasileira-a-tratado-internacional-de-cibercrimes-198233/. Acesso em: 20\11\2021.

CONSIDERAÇÕES FINAIS

A presente pesquisa conseguiu alcançar os objetivos estabelecidos para seu desenvolvimento, tendo sido materializada a dificuldade do Poder Judiciário em punir os agentes que cometem crimes no âmbito virtual. Essas adversidades enfrentadas na fase das investigações, principalmente no que diz respeito a real identificação do autor é um dos maiores problemas dos crimes cibernéticos, pois, é indispensável para que a pretensão punitiva seja justa e direcionada, conhecer quem realmente violou aos preceitos jurídicos preconizados na legislação.

Ainda, foi apresentada a deficiência do ordenamento jurídico brasileiro no que concerne a tipificação dos crimes cibernéticos. Essa falha acarretou diversos impactos para sociedade, no entanto, pode-se dizer que com o advento da Lei nº 14.155/2021 parte dessa preocupação acabou, já que, está dispôs de diversas normas jurídicas relativas aos crimes virtuais, as quais foram incorporadas no Código Penal e no Código de Processo Penal.

Vale ressaltar que, com o avanço das tecnologias e com o aceite da internet pela sociedade, estas ganharam espaço não só nos lares das famílias brasileiras, mas em todo o mundo, no entanto, juntamente com os benefícios trazidos por estas ferramentas sucederam os malefícios. A criminalidade virtual é um dos prejuízos que atingiu a sociedade informatizada, e é a respeito destes que a presente obra convencionou.

Diante do crescimento dos crimes virtuais, surge a necessidade de maior empenho da polícia nas investigações destes e consequentemente a punição dos delinquentes, no entanto, o crime cibernético é complexo e diversas vezes exige perícia especializada em respectivos conjuntos probatórios, estes dedicados a evidenciar a autoria. A perícia especializada também foi um dos obstáculos apresentados, já que, a polícia judiciária brasileira conta com um número baixo de delegacias especializadas, bem como de profissionais competentes para a realização destas perícias.

Ante todo o exposto, nota-se que muitos são os embaraços enfrentados para conseguir de fato, através de provas concretas, definir quem são os autores desses delitos, diante da falta de especialidade e ainda, da facilidade que os criminosos possuem em manter o anonimato através do uso de identificações falsas.

Uma luz surgiu com a Convenção sobre crime cibernético, o Brasil foi convidado para fazer parte deste tratado internacional que dispõe de normas a respeito dos crimes cibernéticos. Esta convenção preconiza que os países signatários colaborem entre si nas investigações de tais crimes, visto que, estes estão quebrando fronteiras e diversos países sofrem com a alta de tal. Atualmente, criminosos cibernéticos são capazes de obter vantagens indevidas mesmo estando do outro lado do continente.

Em outubro do presente ano, a Câmara dos Deputados aprovou a incorporação da Convenção á legislação brasileira, no entanto, para que isso ocorra é necessário passar por apreciação e votação no Senado Federal. Obviamente que este tratado não trará o fim da criminalidade cibernética, mas irá facilitar, o desempenho dos agentes envolvidos no descobrimento da autoria do delito.

REFERÊNCIAS

Advocacia Direito Digital e Crimes Cibernéticos. **Primeiros casos interessantes de crimes na internet.** JusBrasil. Disponível em: https://fernandocbrizola.jusbrasil.com.br/artigos/393077456/primeiros-casos-interessantes-de-crimes-na-internet. Acesso em: 15\11\2021.

AZEVEDO, Leticia Silva de, CARDOSO, Thais Mariana. **Crimes cibernéticos: evolução e dificuldades na colheita de elementos da autoria delitiva**. Disponível em: Disponível em: https://repositorio.animaeducacao.com.br/handle/ANIMA/14146. Acesso em: 20\11\2021.

BENAKOUCHE, Tamara. **Redes técnicas /redes sociais: a pré-história da Internet no Brasil**. Revista USP, São Paulo (35): 124-133, setembro/novembro,1977.

BRASIL. **Código Civil (2002).** Título V- Da prova. Art. 225. Disponível em: https://corpus927.enfam.jus.br/legislacao/cc-02. Acesso em: 20\11\2021.

BRASIL. **Código de Processo Penal (1941).** Capítulo I- Da competência pelo lugar da infração. Art. 70. Disponível em: https://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del3689Compilado.htm. Acesso em: 15\11\2021.

BRASIL. **Código de Processo Penal (1941).** Capítulo I- Da competência pelo lugar da infração. Art. 70§4º. Disponível em: https://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del3689Compilado.htm. Acesso em: 15\11\2021.

BRASIL. **Código Penal (1940).** Título I- Parte Geral, Da aplicação da Lei Penal, art. 1º. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm. Acesso em: 15\11\2021.

BRASIL. **Código Penal (1940).** Parte Geral- Título I- Da aplicação da Lei Penal. Art. 5º. Disponível em: http://www.planalto.gov.br/ccivil_03/Decreto-lei/Del2848compilado.htm. Acesso em: 20\11\2021.

BRASIL. **Código Penal (1940).** Parte Geral- Título I- Da aplicação da Lei Penal. Art. 6º. Disponível em: http://www.planalto.gov.br/ccivil_03/Decreto-lei/Del2848compilado.htm. Acesso em: 20\11\2021.

BRASIL. **Código Penal (1940).** Seção IV- Dos crimes contra inviolabilidade dos segredos, art. 154-A. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm. Acesso em: 15\11\2021.

BRASIL. **Código Penal (1940).** Título II- Dos crimes contra o patrimônio. Capítulo I- Do furto. Art. 155§4º-B §4ª-C. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto lei/Del2848compilado.htm. Acesso em: 15\11\2021.

BRASIL. **Código Penal (1940).** Capítulo VI- Do estelionato e outras fraudes, art. 171. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm. Acesso em: 15\11\2021.

BRASIL. **Código Penal (1940).** Capítulo VI- Do estelionato e outras fraudes. Art. 171§2º-A §2º-B. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto lei/Del2848compilado.htm. Acesso em: 15\11\2021.

BRASIL. **Constituição Federal (1988).** Título II- Dos Direitos e Garantias Fundamentais. Capítulo I- Dos Direitos e Deveres individuais e coletivos, art. 5º, XXXIX. Disponível em: https://www.planalto.gov.br/ccivil_03/Constituicao/ConstituicaoCompilado.htm. Acesso em: 15\11\2021.

BRASIL. Ministério Público Federal. **Crimes cibernéticos: coletânea de artigos.** Brasília, MPF, 2018, 3ª ed., p. 36.

Câmara aprova adesão brasileira a tratado internacional de cibercrimes. Disponível em: https://canaltech.com.br/seguranca/camara-aprova-adesao-brasileira-a-tratado-internacional-de-cibercrimes-198233/. Acesso em: 20\11\2021.

CÂMARA DOS DEPUTADOS (Brasil). Congresso Nacional. **CPI - Crimes cibernéticos: comissão parlamentar de inquérito destinada a investigar a prática de crimes cibernéticos e seus efeitos deletérios perante a economia e a sociedade neste país.** Brasília: 2016. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=214D61B364D3F74027CAB7F56C3E0C39.proposicoesWeb2?codteor=1455189&filename=REL+4/2016+CPICIBER+%3D%3E+RCP+10/2015. Acesso em: 15\11\2021.

CARVALHO, Juliano Mauricio de; ARITA, Carmem Harumi; NUNES, Alesse de Freitas. **A política de implantação da Internet no Brasil.** Disponível em: http://www.portcom.intercom.org.br/pdfs/5be0d57f5fde664d948d9c2cbc80b619.PDF. Acesso em: 25/10/2021.

Convenção sobre cibercrime. Disponível em: http://mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf. Acesso em: 20\11\2021.

Delegacia Interativa registra aumento de mais de 200% em crimes de estelionato por meio da internet. **Governo do Estado do Amazonas**. Disponível em: http://www.amazonas.am.gov.br/2020/06/delegacia-interativa-registra-aumento-de-mais-de-200-em-crimes-de-estelionato-por-meio-da-internet/. Acesso em: 25/10/2021.

Denúncias de crimes cometidos pela internet mais que dobram em 2020. **G1**. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/02/09/numero-de-denuncias-de-crimes-cometidos-pela-internet-mais-que-dobra-em-2020.ghtml. Acesso em: 25/10/2021.

FILHO, Paulo Roberto Aguiar de Lima. **O Direito Penal na quarta revolução industrial: a expansão razoável frente aos crimes cibernéticos**. Delictae, Vol. 6, nº 10, Jan-Jun. 2021.

FILHO, Sergio Cavalieri. **Programa de Sociologia Jurídica**. 15. ed. – São Paulo: Atlas, 2019.

FONSECA, Jaqueline. **Registros de golpes na internet crescem 310% no DF durante a pandemia**. Correio Braziliense, 2020. Disponível em: https://www.correiobraziliense.com.br/cidades-df/2020/08/4868977-mais-golpes-na-pandemia.html. Acesso em: 25/10/2021.

FLORIANO, André Luiz. RODRIGUES, Cláudia Helena do Vale Pascoal. **Crimes informáticos: dos delitos e dos infratores**. Diálogo e interação. Volume 11, n.1 (2017) - ISSN 2175-3687.

FUCHS, Pedro Henrique Camargo; STUANI, Willian Ricieri Dias. **Crimes cibernéticos e a legislação brasileira.** Anuário pesquisa e extensão UNOESC, São Miguel do Oeste, 2021. Disponível em: https://unoesc.emnuvens.com.br/apeusmo/article/download/27927/16295. Acesso em: 25/10/2021.

GRIZOTTI, Giovani. **Golpes e crimes virtuais aumentam durante a pandemia no RS.** G1, 2020. Disponível em: https://g1.globo.com/rs/rio-grande-do-

sul/noticia/2020/06/15/golpes-e-crimes-virtuais-aumentam-durante-a-pandemia-no-rs.ghtml. Acesso em: 25/10/2021.

GOUSSINSKY, Eugenio. **Crimes digitais têm forte alta em vários estados; saiba como prevenir.** Portal R7, 2021. Disponível em: https://noticias.r7.com/tecnologia-e-ciencia/crimes-digitais-tem-forte-alta-em-varios-estados-saiba-como-prevenir-05052021. Acesso em: 25/10/2021.

GUEIROS, Guilherme. NUNES, Eliane**. Lei dos "crimes cibernéticos" altera competência em caso de estelionato.** Conjur. Disponível em: file:///D:/Users/SEVEN/Downloads/ConJur%20-%20Opini%C3%A3o_%20Lei%20dos%20'crimes%20cibern%C3%A9ticos'%20e%20compet%C3%AAncia%20no%20estelionato.pdf. Acesso em: 18\11\2021.

JESUS, Damásio de. Atualização André Estefam. – **Direito Penal**. vol. 1-37. ed. – São Paulo: Saraiva Educação, 2020.

JUNIOR, Janary. **Projeto aprova adesão do Brasil á convenção europeia sobre crime cibernético**. Disponível em: https://www.camara.leg.br/noticias/779447-projeto-aprova-adesao-do-brasil-a-convencao-europeia-sobre-crime-cibernetico/. Acesso em: 20\11\2021.

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

LÉVY, Pierre. **Cibercultura**. 34 ed.- São Paulo, 1999, 264 p. {Coleção TRANS}.

MIRABETE, Julio Fabbrini. **Manual de direito penal: parte especial: arts. 121 a 234-B do CP** – volume 2 / Julio Fabbrini Mirabete, Renato N. Fabbrini. – 36. ed. – São Paulo: Atlas, 2021

MOREIRA, Rafaela. **Golpes virtuais aumentam quase 50% em MS na pandemia; saiba como se proteger**. Correio do Estado, 2021. Disponível em: https://correiodoestado.com.br/cidades/golpes-virtuais-aumentam-quase-50-em-ms-na-pandemia/385464. Acesso em: 25/10/2021.

MOREIRA, Rômulo de Andrade. **A nova competência criminal para o crime de estelionato e a questão dos processos pendentes**. Empório do Direito. Disponível em: https://emporiododireito.com.br/leitura/a-nova-competencia-criminal-para-o-crime-de-estelionato-e-a-questao-dos-processos-pendentes. Acesso em: 15\11\2021.

MOZART, Santos Pedro. **Denunciar crimes virtuais: lista de delegacias especializadas**. Disponível em: http://santospedro.com.br/quero-denunciar-crimes-virtuais-lista-de-delegacias-especializadas/. Acesso em: 20\11\2021.

NUCCI, Guilherme de Souza. **Curso de direito penal: parte geral: arts. 1º a 120 do código penal**. –5. ed. – Rio de Janeiro: Forense, 2021.

NUCCI, Guilherme de Souza. **Manual de Processo Penal**. – 2. ed. – Rio de Janeiro: Forense, 2021.

PINHEIRO, Patrícia Peck. **Direito digital.** São Paulo, Saraiva, 2016, 6ª ed.

PINHEIRO, Patricia Peck. FILHO, Genival Silva Souza. SHINOHARA, Luciane. AVANÇO, Rafaella. **A nova lei de combate às fraudes eletrônicas.** Migalhas. Disponível em: https://www.migalhas.com.br/depeso/347511/a-nova-lei-de-combate-as-fraudes-eletronicas. Acesso em: 15\11\2021.

PRADO, Luiz Regis. **Tratado de direito penal brasileiro: parte especial (arts. 250 a 361)**, volume 3/Luiz Regis Prado. – 3. ed. – Rio de Janeiro: Forense, 2019.

RAMOS, Eduardo Dulcetti. **Crimes cibernéticos: análise evolutiva e legislação penal brasileira**. Disponível em: file:///D:/Users/SEVEN/Downloads/EDRamos.pdf. Acesso em: 20\11\2021.

REALE, Miguel. **Lições preliminares de direito**. São Paulo: Saraiva, 2002.

ROSSINI, Augusto. **Informática, Telemática e Direito Penal**. São Paulo: Memória Jurídica. 2004.

SILVA, Ângelo Roberto Ilha da. **Crimes cibernéticos: racismo, cyberbullying, deep web, pedofilia e pornografia infantojuvenil, infiltração de agentes por meio virtual, obtenção das provas digitais, nova lei antiterrorismo, outros temas.** Porto Alegre: Livraria do Advogado, 2018, 2ª ed.

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

SCHMITT, **Guilherme. Crimes cibernéticos.** 2014. Disponível em: https://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos#:~:text=Da%20Autoria,indevido%20de%20suas%20senhas. Acesso em: 20\11\2021.

SOARES, Gabriella; BUSS, Gabriel. **Em 1 ano de pandemia, tecnologia se torna central para a vida do brasileiro**. Poder 360, 2021. Disponível em: https://www.poder360.com.br/coronavirus/em-1-ano-de-pandemia-tecnologia-se-torna-central-para-a-vida-do-brasileiro/. Acesso em: 25\10\2021.

TOLEDO, Francisco de Assis. **Princípios básicos do direito penal**, São Paulo: Saraiva p.80. In Fernando Galvão e Rogério Greco, Estrutura Jurídica do Crime. Belo Horizonte: Mandamentos. 1999.

Uso de internet, televisão e celular no Brasil. **IBGE Educa Jovens**. Disponível em: https://educa.ibge.gov.br/jovens/materias-especiais/20787-uso-de-internet-televisao-e-celular-no-brasil.html. Acesso em: 25\10\2021.

VIANA, Túlio, MACHADO, Felipe. **Crimes Informáticos**. Belo Horizonte: Editora Fórum, 2013.

VIEIRA, Eduardo. **Os bastidores da internet no Brasil**.- Barueri, SP: Manole, 2003.

WENDT, E.; JORGE, H. V. N. **Crimes Cibernéticos: ameaças e procedimentos de investigação**. Rio de Janeiro: Brasport Livros e Multimídia, 2012.