Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

EDUARDO ROSA PINCERATI

INQUÉRITO POLICIAL NOS CRIMES VIRTUAIS

Assis/SP
2018

Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

EDUARDO ROSA PINCERATI

INQUÉRITO POLICIAL NOS CRIMES VIRTUAIS

Trabalho de Conclusão apresentado ao curso de Direito do Instituto Municipal de Ensino Superior de Assis – IMESA e Fundação Educacional do Município de Assis – FEMA, como requisito parcial à obtenção do Certificado de Conclusão.

Orientando: Eduardo Rosa Pincerati
Orientador: Leonardo de Gênova

Assis/SP
2018

FICHA CATALOGRÁFICA

PINCERATI, Eduardo Rosa.
Inquérito Policial dos Crimes Virtuais / Eduardo Rosa Pincerati. Fundação Educacional do Município de Assis –FEMA – Assis, 2018.

53p.

Orientador: Ms. Leonardo de Gênova
Trabalho de conclusão do curso (Direito) – Fundação Educacional do Município de Assis – FEMA, 2018.

1.Inquérito Policial. 2. Crimes Virtuais.

CDD: 341.432
Biblioteca FEMA

INQUÉRITO POLICIAL NOS CRIMES VIRTUAIS

EDUARDO ROSA PINCERATI

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso de Graduação, avaliado pela seguinte comissão examinadora:

Orientador: _____
Leonardo de Gênova

Examinador: _____
Fernando Antônio Soares de Sá Junior

Assis/SP
2018

Dedico este trabalho aos meus pais e minha irmã por todo carinho e paciência, à toda minha família e amigos, por toda compreensão durante este período em que me dediquei a este trabalho.

AGRADECIMENTOS

Agradeço primeiramente a Deus, por guiar todos os meus passos durante o curso, me proporcionando muita saúde e força para concluir mais está etapa, ao meu orientador, Leonardo de Gênova por todo incentivo e paciência durante a orientação, sendo fundamental para a conclusão deste trabalho.

A minha mãe Clotilde, meu pai Carlos e minha irmã Taís, que foram os pilares que me sustentaram durante todo esta trajetória e que me deram forças e conforto em todos os momentos.

Aos meus avós, Maria Aparecida e Arlindo, que sempre dedicaram seu tempo e esforço para me ajudar em todos os momentos da minha vida, em especial o saudoso senhor Arlindo, que foi um dos maiores exemplos de caráter e honestidade.

Finalmente, minha namorada e amigos que sempre me apoiaram e foram compreensíveis em todos os momentos, agradeço também os amigos que ganhei ao longo de todo o curso aos quais levarei em meu coração.

Tenha coragem de seguir o que seu coração e sua intuição dizem. Eles já sabem o que você realmente deseja. Todo resto é secundário.

Steve Jobs

RESUMO

O presente trabalho faz uma análise dos crimes virtuais através da ótica do inquérito policial, abordando a história da internet e sua evolução até os dias atuais. Trazendo os tipos de crimes mais cometidos dentro da internet, seus reflexos no cotidiano e as formas de investigação utilizadas dentro do procedimento investigatório. Por fim, apresentando também críticas relativas a legislação vigente, problemas e dificuldades durante toda investigação e as possíveis soluções para melhorar os métodos investigativos nesses crimes.

Palavras-chave: Inquérito Policial ; Crimes Cibernéticos

ABSTRACT

The present work analyzes the virtual crimes through the perspective of the police investigation, addressing the history of the internet and its evolution to the present day. Bringing the types of crimes most committed within the internet, their reflections in the daily life and the forms of investigation used within the investigative procedure. Lastly, it also presents criticisms regarding current legislation, problems and difficulties during the investigation and possible solutions to improve investigative methods in these crimes.

Keywords: Police Inquiry; Cyber Crimes

LISTA DE ILUSTRAÇÕES

SUMÁRIO

INTRODUÇÃO

O presente trabalho tem como objetivo analisar os crimes virtuais através da ótica do inquérito policial, estudando o surgimento da internet e sua evolução através dos anos, os crimes que surgiram com o desenvolvimento dessa tecnologia e a conexão do globo criada através da internet.

Com o aperfeiçoamento de tal tecnologia que proporcionou tantos avanços e trouxe consigo vários benefícios ao mundo, também se criou um lado ruim, pois gerou facilidades para criminosos agirem dentro desse espaço denominado internet, eventualmente se utilizando de todos os aspectos benéficos de tal tecnologia para cometer alguns delitos já regulados por nosso ordenamento jurídico, como alguns tipos de fraudes, mas também, se criando novos crimes que surgiram dentro da internet e somente cometidos através dela, como crime de invasão de dispositivo informático.

Dentro do nosso cenário atual e a realidade do nosso sistema jurídico, se faz necessário o desenvolvimento e investimento em novas técnicas de investigação, além de uma adaptação ou até mesmo formulação de novas normas para amparar a aplicação da justiça nesses crimes, pois a internet por ser tratar de uma tecnologia global, que quebrou barreiras e aproximou o mundo é algo a ser estudado mais profundamente e eventualmente regulado de forma mais eficaz para que a impunidade não prevaleça diante desses delitos.

1. A história da internet e as suas ameaças

1.1– A origem da internet

A origem da internet nos remete ao ano de 1946, data na qual foi criado o primeiro computador digital, denominado de ENIAC (ElectronicNumericalIntegratorand Computer ou Computador e Integrador Numérico Eletrônico), feito a pedido do exército do EUA, teve com função realizar cálculos de tabelas balísticas, pesava cerca de 30 toneladas e sua capacidade comparada a nossa tecnologia atual seria a de uma calculadora de mão moderna, conforme o autor Higor Vinicius:

> "Com a finalidade de automatizar o cálculo de tabelas balísticas, no ano de 1946 foi construído o primeiro computador digital, denominado ENIAC, que permitiu reconhecera utilidade universal do invento e passou-se à construção de modelos com mais memória interna e que incorporavam o conceito de programa armazenado, fundamental para a utilização prática da máquina."(Jorge, Higor Vinicius Nogueira, 2017, p.21).

No ano de 1950 começaram a ser produzidos os primeiros computadores comerciais, na qual a empresa IBM (International Business Machines) foi uma das primeiras a começar a produzir tal tecnologia para comercialização, comandando o império da informática até o final 1980. Conforme Jorge, Higor Vinicius:

> "... Elas eram todas diferentes e todas artesanais, mas todas seguiam a chamada arquitetura von Neumann [...] meados da década de 1950 começou a produção dos primeiros computadores comercialmente disponíveis. A IBM saiu na frente neste processo o que lhe valeu o domínio quase absoluto do mercado de informática até meados da década de 1980 [...] ."(Jorge, Higor Vinicius Nogueira, 2017, p.22).

Em 1957 a então chamada União Soviética, com propósitos militares lançou o primeiro satélite artificial, chamado de "Sputnik", com este ato da união soviética, deu-se início a corrida tecnológica entre União Soviética e EUA. Conforme o autor Jorge, Higor Vinicius:

> No ano de 1957 a União Soviética lançou seu primeiro satélite espacial, o Sputnik. A contraofensiva a esse fato foi que o então presidente dos Estados Unidos John Kennedy prometeu enviar um americano para a Lua e criar um sistema de defesa à prova de destruição. (Jorge, Higor Vinicius Nogueira, 2017, p.22).

Com intuito de promover o avanço tecnológico dos EUA na concorrência com a União Soviética, foi criada a ARPA (*AdvancedResearch Project Agency*), contudo no ano que se sucedeu a mesma agência ficou enfraquecida em decorrência da criação da NASA (NationalAeronautics& Space Administration), que basicamente atuava na mesma área e com propósitos parecidos, contudo ligados a outros setores militares.

Após esse enfraquecimento a ARPA, em uma tentativa de melhorar seus números, modificou seu foco de pesquisa principal, realizando parcerias com instituições educacionais como meio de ampliar seu campo de pesquisa, contribuindo para elaboração de novas tecnologias.

No ano de 1962 a força aérea dos EUA, temendo ataques de outros países, solicitou a elaboração de um sistema sofisticado de comunicação militar, quem em tese não teria sistema unicamente central, sendo assim se um de seus terminais de comunicação fosse destruído a comunicação não seria afetada para as demais localidades. Tal sistema foi solicitado à empresa Rand Corporation, que realizou estudos para elaboração desse sistema. Conforme Higor Vinicius:

> No ano seguinte (1962) a Força Aérea, com a preocupação de proteger-se de uma eventual guerra ou ataque nuclear, solicitou à empresa *Rand Corporation* um estudo sobre uma rede de comunicação militar descentralizada3, ou seja, despida de um núcleo central, que funcionasse mesmo que fossem destruídos alguns de seus terminais.(Jorge, Higor Vinicius Nogueira, 2017, p.23).

Com essa ideia a internet começa a engatinhar, um sistema de comunicação em grande escala começava a nascer, contudo após o relatório da Rand Corporation, foi indicado que American Telephone&Telegraph *(AT&T),* fosse responsável por tal sistema, contudo a empresa se negou, pois, tal ideia acabaria por concorrer com seus serviços o que mais tarde isso realmente iria se concretizar.

Com a AT&T fora, a solução para tal projeto ambicioso foi a elaboração de uma rede interligada e sem um núcleo fixo e invulnerável do início, com isso foi criada a ARPANET, que interligava computadores militares sem um centro fixo, através de um sistema de ligações denominadas blackbone (traduzindo para o português “espinha dorsal”).

Mais tarde com a evolução dessa tecnologia e a necessidade de ampliar todo esse sistema, a ARPANET foi liberada para o uso em algumas universidades para se interligarem entre si. De acordo com X (2013, p. 27 *apud* António Cruz):

> "esta agência criou uma rede experimental chamada Arpanet, que utilizava uma tecnologia chamada 'packetswitching' (troca de pacotes) para o transporte de informação, tecnologia esta que é a base do que hoje conhecemos por internet".

Com o desenvolvimento dessa tecnologia que antes era de exclusividade militar e posteriormente liberado o uso para grandes universidades, foi permitido também o uso para empresas.

No ano de 1986 com o desenvolvimento em grande escala nos Estados Unidos a então chamada ARPANET teve uma alteração em seu nome, para o termo que chamamos hoje de INTERNET, tal mudança foi feita pela National Science Foundation, que era a responsável em promover pesquisas no país. Conforme o autor Higor Vinicius:

> "Foi implementado, no ano de 1986, a NSFNET – pela *National Science Foundation* –, e a ARPANET começou a ser chamada de internet."(Jorge, Higor Vinicius Nogueira, 2017, p.25).

Porém o grande avanço que mudaria a INTERNET para o que conhecemos hoje só ocorreu com a criação da WWW (World Wide Web), feita pelos engenheiros Robert Caillaiu e Tim Berners-Lee, a qual revolucionou todo o sistema interligando a rede de computadores mundialmente.

1.2– A história da internet no Brasil

O IBGE (Instituto Brasileiro de Geografia e Estatística) foi um dos primeiros a utilizar o computador a qual foi criado o Centro Eletrônico de Processamento de Dados do Estado do Paraná no ano de 1964.

No ano seguinte o Brasil se associou ao consórcio internacional de telecomunicações via satélite, que alguns anos após desencadeou a criação da empresa de telecomunicações vinculada ao Ministério das comunicações.

Embora o IBGE tenha utilizado o primeiro computador em 1964, o primeiro computador fabricado no Brasil só foi feito em 1972 com o nome um tanto quando peculiar chamado “Patinho Feio”, a responsável por sua criação foi a Universidade Federal de São Paulo (USP).

Nos anos seguintes com a disseminação dessa tecnologia foram criadas empresas, como a Computadores Brasileiros S.A. e secretarias especiais de informática para coordenar os avanços. Porém, o passo mais importante para a internet no Brasil, ocorreu em 1988 com a implementação da internet nas universidades.

Contudo para que a internet no nosso país tivesse uma base sólida para seu desenvolvimento, uma conexão com a internet foi criada através da Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), na qual foi de suma importância para o desenvolvimento de tal tecnologia e de acordo com a revista de pesquisas do próprio site da FAPESP:

> “... A conexão funcionava via linha telefônica ponto a ponto sem necessidade de discagem, por um fio de cobre dentro de um cabo submarino, porque ainda não havia fibra óptica para esse tipo de serviço. Ela era operada pela Academic Network at São Paulo, a Ansp, a rede acadêmica de São Paulo, criada e mantida financeiramente pela FAPESP desde 1988 para suprir a comunicação eletrônica entre as principais instituições de ensino e pesquisas paulistas.” (http://revistapesquisa.fapesp.br/2011/02/18/prim%C3%B3rdios-da-rede_/).

Quando pensamos na internet, já idealizamos em nossa mente o modelo que temos hoje, porém nessa época a internet ainda não possuía os parâmetros de hoje, sua única função basicamente era a de troca de e-mail e se restringia a apenas as universidades para pesquisa. Conforme matéria publicada no site revista pesquisa da própria FAPESP:

> “Não há registro dos conteúdos das primeiras mensagens da internet que chegaram ao Brasil. Getschko e sua equipe não registraram e não lembram o que diziam os primeiros *e-mails*. Para eles, naquele momento tratava-se de mais uma rede a administrar e fazê-la funcionar, e evidentemente todos, inclusive nos Estados Unidos, não tinham noção do sucesso que ela alcançaria dentro de poucos anos.” (http://revistapesquisa.fapesp.br/2011/02/18/prim%C3%B3rdios-da-rede_/).

Mas no ano de 1995, isso acaba mudando, com o aperfeiçoamento dos computadores no mundo, a internet no Brasil começa a ser liberada para o uso comercial e com isso se tem a necessidade da criação do Comitê Gestor da Internet no Brasil (CGI.br). Conforme o site da CGI:

> "A portaria interministerial nº 147 cria o Comitê Gestor da Internet no Brasil (CGI.br)". (https://cgi.br/historicos/#1995).

A sua principal função após sua criação foi coordenar o uso da rede de internet no Brasil e promover o sistema que estava em uma grande expansão, sendo ainda responsável atualmente por toda gestão de nossa rede.

1.3– As primeiras ameaças na internet

As primeiras ameaças a surgirem na internet, foram os hoje denominados vírus auto replicantes, na qual quando infectavam uma máquina se multiplicavam até ao ponto de ocupar grande espaço de sua memória. De acordo com Higor Vinicius Nogueira:

> "No mesmo passo que a evolução dos recursos tecnológicos, as ameaças praticadas via computador se aprimoraram com o passar dos anos. Nesse sentido, a informação sobre programas de computador que se autorreplicassem remonta do final da década de 50, oriunda do matemático John Von Neumann. Na década seguinte surgiramos legítimos antecessores dos códigos maliciosos." (Jorge, Higor Vinicius Nogueira, 2017, p.21).

Esses tipos de vírus surgiram como forma de "jogos" entre programadores, mas, eventualmente foram sendo aprimorados para fins maliciosos à medida que a internet e os computadores evoluíam, contribuindo para a prática de crime nos dias atuais. Conforme cita Higor Vinicius Nogueira:

> "Tudo começou quando um grupo de programadores desenvolveu um jogo chamado Core Wars, capaz de se reproduzir cada vez que era executado, sobrecarregando a memória da máquina do outro jogador. Os inventores desse jogo também criaram o primeiro antivírus, batizado de Reeper, com capacidade de destruir as cópias geradas pelo Core Wars. A existência desse jogo, seus efeitos e a forma de desativá-lo, no entanto, vieram a público somente em 1983, por um artigo escrito por um de seus criadores, publicado em uma conceituada revista científica da época". (Jorge, Higor Vinicius Nogueira, 2017, p.21).

Embora essas ameaças pudessem incomodar o usuário do computador, não geravam grandes danos aos equipamentos, porém, o termo vírus foi apresentado apenas em 1984, de acordo com Nogueira:

> "... em 1984, Fred Cohen apresentou um *paper*, chamado *Experimentswith Computer Viruses*, em que criou o termo "vírus de computador", que denomina programas maliciosos, nocivos ao sistema como um todo." (Jorge, Higor Vinicius Nogueira, 2017, p.22).

O autor também destaca o que é considerado um dos primeiros vírus maliciosos criados, e diz o seguinte:

> "Dois irmãos paquistaneses, no ano de 1986, criaram um vírus de computador chamado *Brain*. Esse vírus atingia o setor de inicialização do disco e tinha como finalidade
> detectar uso não autorizado de um software médico de monitoramento cardíaco que haviam desenvolvido. Porém o código sofreu modificações maliciosas as quais o transformaram em um vírus que se espalhava através de disquetes infectados. O Brain causava lentidão nas operações do sistema e ocupava valiosos kilobytes de memória dos computadores." (Jorge, Higor Vinicius Nogueira, 2017, p.23).

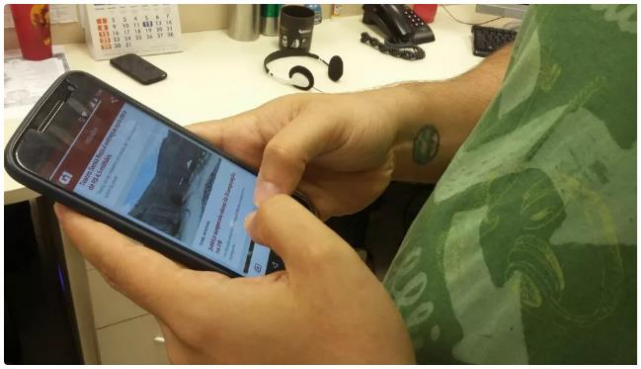
Todas essas ameaças que tiveram suas origens de brincadeiras de programadores ou até mesmo modificação má intencionadas refletiram na tecnologia que temos hoje e nos vírus que acabam por facilitar os crimes cibernéticos, a qual é o foco deste trabalho.

1.4– Internet nos dias atuais

Hoje a internet é uma das ferramentas mais importantes nos dias atuais, sendo praticamente impossível viver sem tal tecnologia. Sua evolução com o passar das décadas nos levou a um patamar de comunicação global, quebrando fronteiras e conectando o globo inteiro com apenas um click.

Várias são as utilidades da internet nos dias de hoje, seja para comunicação entre as pessoas, lazer ou até mesmo trabalho. Isso decorre da facilidade de se comprar um computador ou um aparelho celular com acesso a internet em comparação com anos atrás, desencadeando uma quantidade enorme de acessos a rede mundial de computadores. De acordo com a reportagem do portal G1(2017):

> “Os celulares são responsáveis pela expansão do acesso à internet nos domicílios brasileiros. É o que aponta a Pesquisa Nacional por Amostra de Domicílios Contínua (Pnad), divulgada nesta sexta-feira (24) pelo Instituto Brasileiro de Geografia e Estatística (IBGE). Segundo o levantamento, em 2016 a internet estava presente em 63,6% dos lares e em 94,8% deles havia celulares sendo usados para se conectar à rede.
> Até 2013, menos da metade dos domicílios brasileiros tinham acesso à internet. Somente em 2014 o país ultrapassou a marca de 50% dos lares com conexão à rede.” (https://g1.globo.com/economia/noticia/mais-de-63-dos-domicilios-tem-acesso-a-internet-aponta-ibge.ghtml



Desde 2015, principal meio de acesso à internet no Brasil é o aparelho celular. Em média, há mais celulares que TVs nos domicílios do país. (Foto: Aline Olveira/G1)

Figura 1: usuário convencional brasileiro. Fonte: IBGE

Eventualmente algo maravilhoso como a internet que tanto beneficiou o mundo, começou a ser utilizado para fins maliciosos. Tal ferramenta passou ser uma grande arma na mão de criminosos, seja para facilitar crimes ou até mesmo ocultar outros. De acordo com o site tecmundo(2012):

> “E, infelizmente, o Brasil está entre os três países com maior percentual de vítimas de crimes cibernéticos em relação ao total de habitantes com acesso à rede. O país que lidera o ranking é a China (com 83%), sendo seguido de perto por Brasil e Índia (que empatam em 76%) e dos Estados Unidos (com 73%).” (https://www.tecmundo.com.br/seguranca/32327-76-dos-usuarios-brasileiros-ja-cairam-em-golpes-virtuais.htm).

(Fonte da imagem: Reprodução/Mashable)

Figura 2: imagem do percentual de vítimas. Fonte: Mashable, Tecmundo

O site ainda nos traz a seguintes informações referentes ao prejuízo causado por esses crimes cibernéticos:

> “Por causa de crimes virtuais, estima-se que as empresas de todo o mundo tenham prejuízos que ultrapassam a marca de US$ 1 trilhão (valor que foi atingido em 2008 e pode ter crescido bastante desde então). Para evitar que seu nome faça parte das estatísticas, lembre-se sempre de tomar cuidado com senhas, links e informações cedidas para outras pessoas.”(https://www.tecmundo.com.br/seguranca/32327-76-dos-usuarios-brasileiros-ja-cairam-em-golpes-virtuais.htm).

Com o aumento exponencial do uso, esses números tendem a ser bem maiores atualmente, implicando em sérios problemas jurídicos cotidianamente, além de prejuízos financeiros para empresas e ao particular também. Vale lembrando que grande parte dos usuários habituais da internet não possuem um vasto conhecimento sobre meios de fraudes aplicados na rede mundial de computadores ou até mesmo de procedimentos que possam ser realizados para evitar tais problemas. Contudo tal assunto será abordado nos capítulos seguintes.

1.5– Os crimes cibernéticos

Nas palavras de Higor Vinicius Nogueira os crimes cibernéticos são:

> “... delitos praticados contra ou por intermédio de computadores (dispositivos informáticos, em geral)”. (Jorge, Higor Vinicius Nogueira, 2017, p.34).

Ainda conforme o autor, os crimes cibernéticos se subdividem em 2 grupos, sendo o 1º os denominados “ Ações prejudiciais atípicas”, na qual engloba condutas que embora possam causar algum dano leve ou transtorno a vítima, não irão configurar ou se encaixar em uma tipificação criminal, sendo assim a pessoa que pratica tal ação não poderá ser punido na esfera criminal, um ótimo exemplo exposto por Jorge é:

> "...o indivíduo que invade o computador de um conhecido sem o objetivo de *obter*, *alterar* ou *excluir*dados ou informações ou sem violar um "mecanismo de segurança" não será indiciado nem preso, pois esses fatos não são criminosos, por não se adequarem ao art. 154-A do Código Penal. Por outro lado, o causador do transtorno pode ser responsabilizado na esfera civil, como, por exemplo, ser condenado a pagar indenização em virtude dos danos morais/materiais produzidos".(Jorge, Higor Vinicius Nogueira,2017, p.35)

Neste exemplo, fica claro o exposto pelo autor, pois a tipificação penal acima citada se remete a conduta do agente em invadir um equipamento digital, que tenha ou não acesso a internet para fins de obtenção, adulteração ou destruição de dados.

Muito embora essas condutas classificadas como atípicas não gerem repercussão penal, vale salientar que poderá gerar efeitos na área cível, uma vez que a vítima se achando lesada por tais condutas poderá ingressar com ações de danos morais.

O 2º grupo classificado se refere aos "Crimes cibernéticos", aqui a conduta criminosa existe e possui classificação no texto legal, ou seja, será crime se praticado. Neste segundo grupo o autor faz uma divisão nos crimes, sendo eles de "Crimes cibernéticos abertos" e "Crimes exclusivamente cibernéticos".

Nos denominados "Crimes cibernéticos abertos", o autor nos traz da seguinte maneira:

> "... são aqueles podem ser praticados da forma tradicional ou por intermédio de computadores, ou seja, o computador é apenas um meio para a prática do crime, que também poderia ser cometido sem o uso dele." (Jorge, Higor Vinicius Nogueira, 2017, p.35)

São crimes que para serem consumados não dependem necessariamente da internet, ou seja, o aparato tecnológico serve apenas como ferramenta, pode citar como exemplos crimes como a ameaça, estelionato, pornografia infantil, racismo, crimes contra a honra.

A prática dos crimes citados como exemplo não dependem exclusivamente do meio digital, pois podem ser consumados em diversas formas, porém, podem ser executados no meio virtual.

Já nos "Crimes exclusivamente cibernéticos", conforme Higor Vinicius Nogueira:

> "... são diferentes, pois eles somente podem ser praticados com a utilização de computadores ou de outros recursos tecnológicos que permitem o acesso à internet". (Jorge, Higor Vinicius Nogueira, 2017, p.35)

Aqui o tipo penal descreve a conduta através do meio digital, o exemplo citado pelo autor é:

> "... o crime de aliciamento de crianças praticado por intermédio de salas de bate papo na internet, previsto no art. 241-D do Estatuto da Criança e Adolescente (Lei 8.069/90)". (Jorge, Higor Vinicius Nogueira, 2017, p.35).

No exemplo exposto pelo autor, toda conduta do tipo penal envolve o emprego da internet, sendo necessário para a caracterização do crime. Vário são os crimes que são de exclusividade do meio digital sendo eles: crimes contra a urna eletrônica, interceptação telemática ilegal, entre outros.

Na sua totalidade, os crimes mais comuns no meio virtual, são os contra o sistema financeiro, uma vez que os criminosos para obterem vantagens econômicas se utilizam do ambiente virtual para realizar práticas delitivas como furtos mediante fraude, na qual o agente envia e-mails falsos à vítimas, geralmente com assuntos em que a vítima irá se interessar em abrir, neste momento com a abertura deste e-mail, um vírus infecta o computador e instala programas que irão roubar dados da mesma, se valendo disso o criminoso se utiliza desse dados para seu proveito próprio, podendo obter dados bancários e até mesmo pessoais.

Podemos observar que vários tipos penais foram criados ou interpretados de formas mais ampla em decorrência da criação da internet, os crimes que antes se consumavam na forma tradicional, hoje se encontram no meio digital ou até mesmo em decorrência de novos meios tecnológicos novos crimes surgiram, como é o caso de crimes contra a urna eletrônica, um crime em que anos atrás não existia respaldo no ordenamento jurídico em razão de tal tecnologia não existir ainda. Conforme a citação na obra de Higor Vinicius Nogueira nas palavras de Coriolano Almeida Camargo; temos:

> "Os crimes mais comuns são os cometidos contra o sistema financeiro, os crimes de *phishing*, que são furtos mediante fraude. Uma pessoa recebe uma mensagem falsa, via internet, ela clica no arquivo malicioso e importa um vírus para dentro da máquina. Por exemplo: 'você está sendo notificado porque a Polícia Federal está lhe investigando. Para saber mais detalhes sobre o processo, clique aqui'. No

> momento em que você clica, você importa o arquivo malicioso para dentro da sua máquina, ele vai fazer uma varredura, vai encontrar seus dados bancários e com esses dados ele vai retirar valores da sua conta corrente. Os criminosos descobriram que é muito melhor atacar o correntista, que é o polo mais fraco, do que atacar o polo mais forte, que é o banco. Então, é um crime que utiliza a boa fé, a distração do cliente, não é como o estelionato, em que você entrega espontaneamente as coisas. No furto mediante fraude, a distinção é que a pessoa usa sua distração, você pensa estar clicando em uma mensagem verdadeira – nesse momento é cometida a fraude e, depois, o furto. O furto mediante fraude, dentro do rol de crimes eletrônicos, já está tipificado, ou seja, não precisa de uma legislação para tipificar o furto mediante fraude, mas precisamos de uma legislação para tipificar outros delitos, por exemplo, invasões em portais, em sites, em bancos de dados. Existe uma corrente de juristas que entende que quando você congestiona um serviço público, já existe uma previsão penal por prejudicar o serviço de utilidade pública. Agora, se você prejudicar o serviço de utilidade pública pela internet, talvez você venha a acarretar um dano maior à sociedade. No caso, o delito poderia ser tipificado com uma pena talvez maior, porque as conseqüências para a sociedade também são mais nefastas. Tudo o que acontece no mundo virtual tem propagação nociva mais rápida, tanto para o bem como para o mal. A informação falsa circula mais rápido, e a verdadeira também, pelos meios eletrônicos”

A internet ao mesmo tempo em que nos trouxe grandes benefícios em contrapartida, acarretou diversas situações em que a sociedade teve que se adequar e com isso nosso ordenamento jurídico também, embora essas mudanças efetivamente não tenham cumprido ou resguardado o direito em sua totalidade.

Nesses crimes, o maior desafio muitas vezes não se resume a ausência de leis regulamentadoras somente, mas também a parte investigativa, pois a internet como analisamos no decorrer no capítulo é algo muito grande, o que dificulta muito o trabalho investigativo.

2. Investigação dos crimes virtuais

Após a abordagem dos crimes descritos no capítulo anterior, abordaremos agora as formas de investigações dos crimes virtuais. Para tal temos que entender o inquérito policial, que é a forma com que são iniciadas as investigações para apurar estes crimes.

2.1 – Inquéritos Policiais

A investigação criminal tem início com a instauração do chamado Inquérito Policial pelo delegado da policial judiciária, mas, o que seria o inquérito policial dentro do ordenamento jurídico? Tal indagação é respondida pelo doutrinador Fernando Capez:

> É o conjunto de diligências realizadas pela polícia judiciária para a apuração de uma infração penal e de sua autoria, a fim de que o titular da ação penal possa ingressar em juízo (CPP, art. 4º). Trata-se de procedimento persecutório de caráter administrativo instaurado pela autoridade policial. Tem como destinatários imediatos o Ministério Público, titular exclusivo da ação penal pública (CF, art. 129, I), e o ofendido, titular da ação penal privada (CPP, art. 30); como destinatário mediato tem o juiz, que se utilizará dos elementos de informação nele constantes, para o recebimento da peça inicial e para a formação do seu convencimento quanto à necessidade de decretação de medidas cautelares. (Curso de Processo Penal - Fernando Capez – 2016)

O inquérito tem um papel de suma importância para a apuração dos crimes virtuais, e através dele que todos os procedimentos investigativos serão realizados a fim de constatar os eventuais criminosos, e futuramente poderá ser utilizado em uma eventual ação penal.

2.1.2 - Inquérito Extrapoliciais

Embora boa parte dos inquéritos sejam realizados através da polícia judiciária, não é algo exclusivamente da mesma, o autor Fernando Capez nos traz algumas formas de inquérito extrapolicial:

> O art. 4º, parágrafo único, do Código de Processo Penal deixa claro que o inquérito realizado pela polícia judiciária não é a única forma de investigação criminal. Há outras, como, por exemplo, o inquérito realizado pelas autoridades militares para a apuração de
> infrações de competência da justiça militar (IPM); as nvestigações efetuadas pelas Comissões Parlamentares de Inquérito (CPI), as quais terão poderes de investigação próprios das autoridades judiciais, além de outros previstos nos regimentos das espectivas Casas, e serão criadas pela Câmara dos Deputados e

> pelo enado Federal, em conjunto ou separadamente, ediante requerimento de 1/3 de seus membros, para a apuração de fato determinado, com duração limitada no tempo (CF, art. 58, § 3º); o inquérito civil público, instaurado pelo Ministério Público para a proteção do patrimônio público e social, do meio ambiente e de outros interesses difusos e coletivos (CF, art. 129, III), e que, eventualmente, poderá apurar também a existência de crime conexo ao objeto da investigação;

Todavia, iremos nos fixar exclusivamente nos crimes comuns e na forma de inquérito realizado pela polícia judiciária.

2.1.3 - Polícia judiciária

Outra indagação necessária para melhor compreensão do inquérito policial é a figura da policial judiciária, o que essa figura representa dentro do inquérito e sua função, conforme citação do livro doutrinador Fernando Capez:

> "Conforme Julio Fabbrini Mirabete (*Código de Processo Penal interpretado*, 2. ed.,Atlas, 1994, p. 35), "a Polícia é uma instituição de direito público destinada a manter a paz pública e a segurança individual".

Tal instituição tem um caráter fundamental dentro do nosso sistema jurídico, exercendo o serviço de prevenção e repressão dos crimes que acontecem em nosso cotidiano, ou seja, a chamada paz pública está a cargo da policia judiciária.

2.1.4 – Finalidade

Podemos concluir finalmente que o inquérito policial é chave principal para desvendar esses crimes, trazendo à tona os autores e eventualmente a classificação daquele crime em nosso ordenamento e que servira como base para o início de uma ação penal.

2.2 – Forma de investigação

Após entendermos o inquérito policial, passaremos agora a forma de investigação, para tal, iremos classificá-la em duas fases conforme o autor Higor Vinicius dá classificação:

> "O importante é que o leitor compreenda que não há nada de mais complexo nesse processo investigativo, somente uma fase inicial, técnica, e uma fase consequencial, de investigação policial propriamente dita. Expliquemos. Para a melhor compreensão do leitor, vamos estabelecer a nominação das duas fases de investigação da seguinte forma: fase técnica e fase de campo".(Jorge, Higor Vinicius,2017, pag. 103)

Ao iniciar as investigações, a mesma é procedida pela 1ª fase, denominada fase técnica, alguns elementos são analisados durante a investigação, tais como finalidade a busca e a localização do computador que foi utilizado para prática do crime virtual, para tal analisaremos algumas tarefas a serem realizadas neste procedimento, a qual é descrita pelo autor Higor Vinicius como:

> "•análise das informações narradas pela vítima e compreensão do fato ocorrido na internet;
> •orientações à vítima com o intuito de preservar o material comprobatório do delito e a sua proteção virtual;
> •coleta inicial de provas em ambiente virtual;
> •formalização do fato criminoso por intermédio de um registro ou boletim de ocorrência63, com a consequente instauração do feito;
> •investigação inicial referente aos dados disponíveis na rede mundial de computadores sobre prováveis autores, origem de e-mails, registro e hospedagem de domínios;
> •formalização de relatório ou certidão das provas coletadas e apuração
> •preliminar64;
> •representação perante o Poder Judiciário para expedição de autorização judicial para quebra de dados, conexão ou acesso. Também poderão ser solicitados os dados cadastrais para os provedores de conteúdo.
> •análise das informações prestadas pelos provedores de conexão e/ou provedores de conteúdo." (Jorge, Higor Vinicius, 2017, pag. 103)

Tais tarefas influenciam de forma substancial a investigação, para que se possamos passar para a segunda fase da investigação, contudo, vamos abordar cada tarefa a fim de entender sua função para tal procedimento.

2.2.1 – Informações narradas pela vítima

Os fatos são descritos pelo vitima nos seus mínimos detalhes, nesta fase toda informação prestada pela vitima é de suma importância, aqui será à base da investigação a qual será atribuído o melhor método para iniciar as investigações.

2.2.2 – Orientações à vítima

Objetivo desta fase é preservar todo e qualquer vestígio do crime virtual, sejam e-mails salvos, fotos, textos, áudios, vídeos e etc. Muitas vezes a vítima acaba por medo ou até mesmo motivado por forte emoção, excluindo ou apagando o material comprobatório, dificultando posteriormente a investigação.

2.2.3- Coleta inicial de provas em ambiente virtual

Nesta fase o policial irá colher as primeiras provas para nortear a investigação, se fará com todo material que na fase anterior foi preservado pela vítima, o agente irá salvar todo conteúdo disponível pela mesma e eventualmente analisará toda informação coletada.

2.2.4 - Formalização do fato criminoso

Após as análises dos fatos descritos pela vítima, a coleta das provas dentro do ambiente virtual, o agente irá formalizar todo ato em um boletim de ocorrência para dar início ao inquérito policial. Aqui será atribuído o tipo de crime a ser investigado e sua classificação dentro do Código Penal.

2.2.5 - Investigação inicial

Os atos realizados nessa fase, na sua grande maioria dependem de autorização judicial para que o agente público tenha acesso a informações privilegiadas, isto decorre do sigilo imposto por lei as empresas, para preservar a integridade dos usuários. Um exemplo disso são as empresas de telefonias que para divulgarem dados de um cliente, se faz necessária uma autorização judicial para que seja disponibilizado os dados.

2.2.6 - Formalização de relatório

As provas coletadas no decorrer da investigação, nesta fase serão formalizadas dentro do inquérito policial, provas documentais são anexadas ao inquérito, sempre respeitando as formalidades legais.

2.2.7–Preliminar

Aqui são apresentados preliminarmente os fatos da investigação que irão desencadear a ação penal. Vale salientar que nesta fase não existe o contraditório e nem ampla defesa, apenas é feita a investigação pelo modo inquisitivo.

2.2.8 - Representação perante o Poder Judiciário

Esta fase poderá ser antecipada conforme o decorrer da investigação, pois se tratando de alguns casos a urgência para identificação de contas ou pessoas antes que elas se ocultem ou apague seus rastros.

2.2.9 - Análise das informações prestadas pelos provedores de conexão

Todas as informações obtidas dos provedores passam a ser analisadas pelos agentes de policia, descartando informações desnecessárias que não irão contribuir com a investigação. E eventualmente formalizando as provas necessárias a investigação.
Neste ponto vale salientar que a uma grande dificuldade na maioria das vezes, pois atualmente muitos usuários e inclusive criminosos acabam por ocultar sua navegação dificultando assim a localização do usuário.

2.2.10 Segunda fase da investigação

Finalizada a primeira fase da investigação, após devidamente localizado o dispositivo eletrônico que foi utilizado para a prática do crime, será iniciada a segunda fase, denominada fase de campo, aqui serão realizados diligência para coletar mais provas, conforme e dito pelo autor Higor Vinicius Nogueira:

> "A partir da identificação e localização do computador que permitiu a conexão e o acesso criminoso na internet surge a denominada fase de campo, quando há necessidade de deslocamento de agentes policiais para realização de diligências com o intuito de promover o reconhecimento operacional no local." (Jorge, Higor Vinicius, 2017, pag. 103)

Vale destacar que essa fase tem que ser feita de forma cuidadosa, já que determinados atos devem ser feitos mediante autorização judicial, ou seja, respeitando a forma legal, para que eventualmente evitar que a prova coletada seja descartada por ter sido produzida de forma ilegal.
Um exemplo clássico disto é a busca e apreensão, para que os policiais possam adentrar em determinada residência e prender pessoas ou apreender objetos como provas, uma autorização judicial se faz necessária.
Outro exemplo que o autor Jorge, Higor Vinicius Nogueira nos traz neste contexto da investigação é:

> "Outra circunstância que poderá derivar da análise dos documentos é a solicitação ao Poder Judiciário para que determine ao administrador de rede de determinado local que preste informações específicas e técnicas que visem indicar diretamente a máquina de onde partiu o acesso." (Jorge, Higor Vinicius,2017, pag. 103)

Este caso citado pelo autor, diz respeito as redes comerciais em que, várias pessoas utilizam a mesma rede e se faz necessário informações pessoais do administrador para identificar de forma específica o usuário que cometeu o crime.

2.3 – Investigações em sites

As investigações que tem como objetivo os sites na internet, acabam por se tornar algo um pouco complexo e dificultoso, haja visto que, embora quando acessamos uma página da web ela venha naquele formato que estamos acostumados, o registro do mesmo se dá através do chamado domínio (espécie de registro ou identificação virtual na internet.), conforme nos traz o autor Higor Vinicius:

> ”Para o usuário comum não são visíveis detalhes sobre a programação de acesso a um site. O usuário de computador digita o endereço no seu navegador e as informações do site aparecem na tela. No entanto, quando há a digitação de um endereço de um domínio na barra de endereços do *browser*, ocorre automaticamente a tradução para um endereço numérico, função que é realizada pelo servidor DNS (*Domain Name System*), correspondente a um sistema de nome e domínio.
> Por exemplo, ao digitar o endereço do site da Polícia Civil do Estado de São Paulo – www.policiacivil.sp.gov – ocorre a tradução simultânea para o endereço IP 200.144.4.82.” (Jorge, Higor Vinicius,2017, pag. 106)

Algo que fica oculto do usuário convencional, a qual só o programador daquele site tem acesso, nas investigações se faz necessária a localização do dono desse domínio (site), é nesta etapa que a investigação pode complicar, pois e necessário localizar o possuidor do mesmo e eventualmente pode não estar registrado no país.

2.3.1 – Domínios

Como citado anteriormente domínio de um site, funciona em tese como a identidade do mesmo na internet, algo que distingue dos demais.

Tal registro e atualmente regulado pelo Comitê Gestor da Internet, a qual são impostas algumas regras para o registro do domínio dentro do Brasil na qual o autor Higor Vinicius nos traz:

> “Para o usuário criar um site, o primeiro passo é registrar um domínio na internet. O domínio é o endereço (ou URL) do site. No Brasil, tal função é responsabilidade do Comitê Gestor da Internet68 (CGI.br) através do Registro.br69. Tanto pessoas físicas quanto jurídicas poderão registrar um domínio. Pelas regras atuais

> existentes no Brasil, um nome de domínio, para o devido registro, deve estar disponível70.” (Jorge, Higor Vinicius,2017, pag. 106)

Além disso, a CGI.br traz um rol de regras sintáticas para o registro do domínio dentro do país, tudo para diferenciar e tornar fácil a localização, finalidade desse domínio.

2.3.2 – Domínio no exterior

Os domínios de sites feitos fora do Brasil funcionam de forma semelhante, embora, sejam regulados conforme o órgão de cada país. Isto acaba trazendo um grande empecilho nas investigações, uma vez que alguns países para se ter um domínio, basta cadastrar o nome do site e pagar uma taxa devida para efetuar registro, acabando por dificultar em uma eventual instigação, pois, o dono desse domínio acaba ficando no anonimato sendo quase impossível localizá-lo.

2.4 – Armazenamento de provas

Algo muito importante dentro do inquérito policial também, é o armazenamento do conteúdo coletado durante as investigações, em tese os meios de prova são salvos em formas de impressões, contudo, alguns métodos foram desenvolvidos e o autor Jorge Higor Vinicius nos traz em sua obra como tal iremos analisar cada uma.

2.4.1 – Print Screen

Uma ferramenta muito utilizada nos computadores, que funciona como uma câmera que tira foto da tela inteira do computador, exibindo na imagem tirada todo conteúdo que eventualmente estava aberto no momento do procedimento. O autor Jorge, Higor Vinicius ainda destaca:

> “A primeira delas é o **uso da tecla “print screen”**, que copia a imagem que estiver aparecendo na tela. Após clicar “print screen” (ou “Alt” + “print screen” para copiar apenas a janela ativa), o responsável pela coleta cola o conteúdo em algum programa de edição de imagens, como o “paint”, ou de textos, como o Word ou Writer. Neste último caso, pode integrar um relatório da investigação inicial feita ou, no caso do advogado, da petição inicial. A utilização tão-somente do procedimento usando “print screen” não é recomendada, pois pode ser questionada judicialmente e não ser aceita como prova do delito, em razão da possibilidade de manipulação, montagem etc. Portanto, deve ser utilizada concomitantemente com outros procedimentos, citados a seguir”.(Jorge, Higor Vinicius,2017, pag. 145)

O próprio autor acaba destacando que este procedimento pura e simplesmente dentro do inquérito é passível de dúvidas em uma eventual ação penal, contudo, tal procedimento deve ser usado em junção com outros meios que serão citados adiante.

2.4.2 – Salvamento de arquivos no navegador

Um procedimento bastante utilizado também, que consiste em salvar o endereço da página pelo próprio navegador, nas palavras de Higor Vinicius:

> "A segunda opção é de **salvamento de cópia das páginas** usando as formas padrão de salvamento de arquivos em .html existentes nos diversos navegadores de internet (browser). Para tal, siga os passos: menu "Arquivo" ou "Ferramentas" ◊"Salvar página como" ◊ "Tipo – Página web, completa"86, sugerindo-se salvar o arquivo em uma pasta criada para tal. Salvando a página serão criados, em regra, dois arquivos, um com o nome da página (o qual se sugere não modificar) e uma pasta com os arquivos vinculados. O problema em relação a esse tipo de opção é que os *links* vinculados não são salvos, tendo-se que adotar o mesmo procedimento a cada *link* que interesse ao processo investigativo. Outro aspecto problemático é que não é gerado nenhum arquivo de log da gravação, e o arquivo .html pode ser manipulado e/ou alterado, sendo importante levar o arquivo a um tabelionato e lavrar uma Ata Notarial."(Jorge, Higor Vinicius,2017, pag. 145)

O próprio autor destaca que esse método não é muito efetivo por conta da perca dos links que muitas vezes são necessários também dentro da investigação.

2.4.3 – Programas

Aqui já passamos a utilizar alguns softwares que ajudam na investigação, com intuito de salvar informações e retirá-las do ambiente virtual, o próprio autor faz menção alguns programas bastante utilizados para tal procedimento:

> "A terceira opção é o **uso conjunto dos programas HTTrack Website Copier e do MD5summer**. O primeiro *software* é uma ferramenta extremamente útil e fácil de ser utilizada, atentando-se para que a cópia seja gerada incluindo-se os *links*vinculados ao site e que interessem à investigação, ou seja, a profundidade e os limites na cópia, já que a cópia da simples máscara do site pode não trazer informações importantes à investigação policial. O próprio *software*, quando da realização da cópia do site, gera um *log* da gravação feita e um arquivo "index", possibilitando-se gravar todo o conteúdo em um CD para ser anexado ao Inquérito Policial e/ou processo judicial. No caso de sites com acesso por login e senha, o HTTrack não pode ser utilizado. Ao final da obra, nos anexos, consta tutorial que contém o passo a passo para a utilização destas ferramentas em conjunto."(Jorge, Higor Vinicius,2017, pag. 145)

Tais softwares se tornaram de suma importância dentro da investigação, uma vez que facilitam a obtenção e armazenamento de provas.

2.4.4 – Ata Notarial

Aqui se trata de uma forma de produção de prova extrajudicial, a qual é feita muitas vezes pela própria vítima ou por seu representante, dentro de um Cartório de Notas, nas palavras do autor:

> A quarta opção é o **registro de uma Ata Notarial**. Pode-se conceituar a Ata Notarial como oinstrumento público através do qual o tabelião ou seu preposto – a pedido de pessoa interessada ou por quem a ela represente – autentica em forma narrativa os fatos, se estado, e tudo aquilo que atesta por seus próprios sentidos sem a emissão de opinião, juízo de valor ou conclusão, portando por fé (pública) que tudo aquilo presenciado e relatado representa a verdade com consignação nos livros de notas87. (Jorge, Higor Vinicius,2017, pag. 145)

Basicamente, o Tabelião ou seu Substituto, irá ver os fatos à ele apresentado e descrever dentro de um documento público o que está presente no documento; um ótimo exemplo de tal procedimento são as atas notariais feitas a partir de análise de redes sociais a qual a vítima pode ter sofrido uma calúnia, difamação ou injúria e queira tornar aquilo como uma prova, antes que o autor de tal delito apague a postagem.

2.4.5 – Certidão da Polícia Civil

A certidão emitida pela polícia civil tem o mesmo princípio da ata notarial, visto que, o Escrivão como o tabelião, possuí a chamada fé pública para redigir e narrar os fatos à ele apresentado. Nas palavras do autor:

> A **certidão elaborada pela Polícia Civil** representa outro importante instrumento. Não seria lógico o Delegado de Polícia ter que imprimir os dados e levá-los a um tabelionato para fins de registro de Ata Notarial. Por isso surge a quinta e última opção de salvaguarda de dados eletrônicos e/ou telemáticos: a certidão elaborada pelo Escrivão de Polícia. O agente policial, na condição de "Escrivão", tem fé pública sobre seus atos e pode, acessando uma página na internet, promover a sua impressão e certificar data e existência. Assim, também pode e deve usar todos os meios disponíveis.(Jorge, Higor Vinicius,2017, pag. 145)

Esses dois últimos meios de provas muitas vezes são utilizados para registrar os fatos de forma efetiva, uma vez que ao depender da situação ou do crime as provas possam sofrer alterações ou até mesmo serem apagadas do ambiente virtual.

Vale salientar que aqui além dos fatos que são apresentados perante ao escrivão, o agente público poderá se utilizar de outras formas de produção de prova para elaboração dessa certidão, como por exemplo salvar os dados por meio de um programa especial.

2.5 – Investigação de cibergolpes

Um termo novo utilizado dentro do meio investigativo que diz respeito as formas de golpes ou fraudes realizadas no ambiente virtual. Esta pratica tem se elevado constantemente devido a especialização de criminosos nessas áreas, visto que, diferente dos golpes aplicados diretamente a vítima que são eventualmente menos efetivos,os golpes no meio digital na sua maioria têm uma maior taxa de sucesso, além disso o criminoso possui uma gama enorme para operar e uma infinidade de aparatos e programas que o ajudem a cometer tais delitos, além de ocultar seus rastros, dificultando eventualmente sua localização.

Outro fato que contribui também para aumento dessa pratica, é a disseminação da internet pelo mundo, além de sua imprescindível necessidade no nosso cotidiano. O mundo hoje se tornou escravo dessa tecnologia, sendo que alguns setores sem essa tecnologia não funcionam, causando um grande caos em sua eventual falta.

2.5.1 – Fraudes

Para entendermos o que são os chamados cibergolpes na sua integralidade, devemos entender primeiramente o conceito de FRAUDE, na citação do autor Higor Vinicius Nogueira:

> “SANTOS (2008) define fraude como osubterfúgio para alcançar um fim ilícito, ou ainda, o engano dolosamente provocado, o malicioso induzimento em erro ou aproveitamento de preexistente erro alheio, para o fim de enriquecimento ilícito.” (Jorge, Higor Vinicius, 2017, pag. 148)

Podemos observar que o criminoso se aproveita muitas vezes do erro da vítima ou a induz ao erro dolosamente, para obter essa vantagem ilícita sobre ela.

Além disso, podemos nos utilizar do próprio conceito dentro do nosso Código Penal, que consagra vários tipos de fraude, mas tomamos como exemplo o artigo 171 do Código Penal Caput, que será à base dos crimes de fraudes que iremos tratar, na qual nos traz a seguinte redação:

> **Estelionato**
> 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. (http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm).

A própria redação da lei já estabelece que a forma de cometer este tipo de crime, na qual engloba qualquer artifício, ardil ou meio fraudulento que enseje vantagem ilícita em cima de terceiro, ou seja, o meio digital é utilizado nesse caso para cometer esse crime.
Mas o que seria a chamada fraude eletrônica, de acordo com o autor Higor Vinicius :

> "Em face da amplitude que o conceito de "fraude eletrônica" abrange, no decorrer deste livro o assunto será delimitado aos dois tipos de fraudes mais comuns dentre aquelas praticadas em ambiente virtual, quais sejam: fraudes relacionadas com o comércio eletrônico, mais especificamente os "sites fraude"96, e os sites de falsos empréstimos. Nos demais, a lógica de apuração e investigação é bastante similar."(Jorge, Higor Vinicius,2017, pag. 148)

Vamos analisar os dois tipos de fraudes e seu procedimento de investigação dentro do inquérito policial.

2.5.2 – Sites fraudes de comércio

Sites que tem como objetivo ludibriar o usuário, lhe ofertando produtos ao um preço que lhe chame a atenção e ofereça vantagem econômica alta para o mesmo.
Na sua grande maioria são sites falsos que nem ao menos possuem uma loja física, tudo o que está a mostra na página é meramente um chamariz para o usuário, ele simula a venda de um produto ao usuário e o mesmo nunca terá o seu produto em mãos.
Essa prática tem aumentado muito atualmente, uma vez que o comércio via internet e sites de compra são atualmente uma das melhores formas de adquirir um produto.
Para entendermos este tipo de crime, vamos analisar suas características, nas palavras do autor Higor Vinicius Nogueira

> **"•Criação de domínios e hospedagem no Brasil ou exterior**
> **•Indexação em sites de pesquisa de preços:**
> **•Suposta confiabilidade inicial à condição de legalidade e credibilidade do site:**
> **•Preço oferecido pelo site fraude é abaixo da média de outros sites de e-commerce:**
> **•O pagamento exigido, em regra, é à vista, por boleto ou depósito bancário em contas de pessoas físicas:**
> **•Sites fraude não possuem Política de Privacidade e Termos de Uso ou os têm bastante reduzidos:**
> **•Quando informado o CNPJ, a empresa é de fachada:**

•Poucas formas de contato com os responsáveis pela empresa:”

Os criminosos muitas vezes acabam registrando o domínio do site no exterior para fugir de algumas regras impostas pela CGI.br, para ocultar sua localização e facilitar o crime.
Efetuam publicidade do site, para ter um maior alcance de vítimas, para isso cadastrando o domínio em sites de busca de preço.
O preço oferecido sempre será um chamariz para a vítima, uma vez que para atraí-las colocam muitas vezes bem abaixo da média oferecido em demais sites, causando a vítima uma sensação de vantagem por estar adquirindo o produto.
As formas de pagamento na sua grande maioria vão ser de uma forma com que o fraudador tenha posse integral e rápida da vantagem econômica, evitando outros meios que possibilitem sua localização, como o parcelamento em cartões de crédito.
Políticas de privacidade, muitas vezes ignoradas no momento em que nos cadastramos em alguns sites, são muito importantes, pois em sites falsos os fraudadores acabam não se atentando muito a este tipo de detalhe, de forma que acabam por colocar de forma errônea ou até mesmo não colocando.
O CNPJ muitas vezes será de fachada, não possuindo endereço correto ou até mesmo endereços falsos e em alguns casos o CNPJ que consta no site poderá ser invalido estando ali somente para passar sensação de algo valido.
Esses sites na sua grande maioria evitam contatos com suas vítimas, para tal fornecem números descartáveis ou contatos errados, tudo para evita uma eventual localização.

2.5.2.1 – Investigação

Neste tipo de crime alguns procedimentos especiais são adotados no momento da investigação, o autor Higor Vinicius em sua obra cita cinco passos para investigação, das quais irei discorrer a respeito:

a) Registrar todo o conteúdo deste site através das formas de obtenção e arquivamentos de provas citados ao longo do capitulo;
b) A vítima se possível trará para o delegado, para incluir no inquérito todas as provas que possua, sejam elas em formas de mensagens, imagens ou número de telefones trocados com o fraudador do site;
c) Algo muito importante, a verificação do domínio, na qual boa parte das informações do fraudador podem sem obtidas através do seu cadastro de domínio;
d) Hospedagem do site, ou seja, empresa responsável por manter o site no ar, aqui se tem o cuidado, pois para acessar tais informações dessas empresas se faz necessário um mandado judicial;

e) Todos os dados obtidos durante a investigação serão utilizados para localizar o fraudador, seja na pesquisa do domínio, bloqueio de contas que foram efetuados o deposito, além de demais procedimentos que o delegado de polícia possa solicitar nesse passo para ajudar nas investigações, como quebra de sigilo bancário, telefônico, grampear telefones e etc.

Estes procedimentos na sua grande maioria são efetivos, embora, a polícia civil encontre sérios problemas durante a investigação, contudo, tal assunto será abordado de forma integral no capítulo seguinte.

2.5.3 – Sites de Falsos Empréstimos

Embora grande parte das fraudes sejam realizados por meio de sites de compras, uma outra pratica muito utilizada pelos fraudadores são sites de falsos Empréstimos, na qual tem como principal objetivo, oferecer empréstimos altos aos seus “clientes”, e em contrapartida apenas cobrar um valor de “garantia” para realizar tal transação.

A maioria das vítimas desse tipo de golpe, por se encontrarem muitas vezes com problemas financeiros, em seu desespero, acabam se encantando com esses tipos de ofertas feitos por esses sites e acabam realizando o “empréstimo” e depositando a quantia exigida pelo fraudador no site.

Em relação as suas características, elas basicamente são iguais aos de sites falsos de comércio, partem do mesmo princípio, somente alterando seu modo de aplicar e efetivar a fraude, vale lembrar que a maioria desses sites também se utilizam de imagens de instituições conhecidas, induzindo a vítima a uma falsa sensação de segurança no momento da transação.

2.5.3.1 – Investigação

Sua linha investigativa é a mesma dos sites de fraude comercio, contudo, boa parte da investigação e focada no domínio desses sites, e eventualmente a contas anexadas a ele, pois na sua grande maioria se tratam de valores altos e grandes movimentações bancárias, exigindo assim uma ampla investigação no que diz respeito a essas movimentações, localizando os proprietários, solicitação do delegado para a quebra do sigilo de contas e etc.

O autor Higor Vinicius, destaca alguns cuidados que os usuários devem ter ao acessar esses sites:

> 1.Se o site contém ou não menção quanto à atividade *factoring* e com autorização do Banco Central do Brasil;
> 2.Se o site contém, no contrato disponibilizado online, qualquer menção ao CNPJ da empresa, procurando pesquisá-lo para ver se corresponde à instituição bancária informada;
> 3.Se o site possui autorização para funcionar como estabelecimento que ofereça créditos;
> 4.Se o site possui endereço(s) fixo(s) informado(s) como sendo a sede e/ou a filial da instituição financeira;
> 5.Se o site possui *política de privacidade e termos de uso*118;
> 6.Se for possível, verificar se o domínio está registrado em nome de pessoa física ou jurídica;
> 7.Se o site contém algum indicativo de contato facilitado com clientes, conforme exige o CDC119;
> 8.Efetivar pesquisa nos sites de reclamação anteriormente citados e outros de sua confiança;
> 9.Na dúvida, contatar a instituição financeira através de outro meio que não os informados no site em suspeição;
> 10.Por fim e mais importante, procurar sempre fazer empréstimo junto a uma instituição bancária cujo endereço é real e não virtual, e cujo contrato é fornecido pessoalmente por colaboradores e/ou gerentes. (Jorge, Higor Vinicius,2017, pag. 170)

Cuidados importantes que os usuários devem tomar para evitar esses tipos de golpes aplicados na internet, evitando assim transtornos e percas patrimoniais altas.

2.6 – Tipificação

A tipificação desses crimes, são aplicados na maioria dos casos o artigo 171 do Código Penal, na qual foi citado ao longo do capitulo que seria a base para entendermos esses tipos penais.

Embora se enquadre no artigo 171 do Código Penal, o próprio delegado pode incluir no seu relatório final do inquérito outros tipos penais, como descreve o autor Higor Vincius:

> “Pode o Delegado de Polícia, no decorrer da investigação policial, detectar outros delitos, como geralmente ocorre. Por exemplo, é comum a prática destes crimes por quadrilha ou bando, incidindo o art. 288 do Código Penal Brasileiro.”(Jorge, Higor Vinicius,2017, pag. 171).

O fraudador pode além de responder pelo estelionato, poderá também se sujeitar a outros tipos de crimes dependendo de sua conduta no crime.

2.6.1 – Competência da investigação

Em relação à competência da investigação desses crimes, nas palavras do autor Jorge, Higor Vinicius:

> “Cumpre observar algo quanto à atribuição e competência, respectivamente, para investigar e processar autores de estelionato: é do local onde se obteve a vantagem financeira indevida”(Jorge, Higor Vinicius,2017, pag. 171).

Se a vantagem aconteceu na cidade de Paraguaçu Paulista, todo inquérito será realizado por meio da delegacia da mesma, o autor ainda cita em sua obra uma jurisprudência sobre assunto:

> PENAL E PROCESSO PENAL. HABEAS CORPUS. NARRATIVA DE CONDUTA QUE, EM TESE, SE SUBSUME AO ARTIGO 171, CAPUT, C/C ARTIGO 71, DO CÓDIGO PENAL. CRIME DE DUPLO RESULTADO MATERIAL. CONSUMAÇÃO DO ESTELIONATO: OBTENÇÃO DA VANTAGEM PATRIMONIAL EM DETRIMENTO DA VÍTIMA. CHEQUES SACADOS DIRETAMENTE NO CAIXA BANCÁRIO. INDICAÇÃO DO ATO CONSUMATIVO QUE SE FAZ INDEPENDENTEMENTE DE SE SABER SE A VANTAGEM ERA “DEVIDA” OU “INDEVIDA”. JUÍZO COMPETENTE: O DO lUGAR EM QUE SE DERAM OS SAQUES. ORDEM DENEGADA. (Jorge, Higor Vinicius,2017, pag. 172).

Até mesmo os tribunais estão pacificando esse posicionamento em relação aos seus julgados, se aplicando então a investigação.

2.7 – Crimes em Rede Sociais

As redes sociais hoje são um dos principais canais de comunicação global, e com isso virou alvos de criminosos dentro delas, quando me refiro as redes sociais, podemos citar o Facebook, Instagram, Twitter, Tumblr,Whatsapp, entre outras muitas existentes pela internet e que possuem milhões de usuários diariamente.

2.7.1 – Tipos de crimes nas Redes Sociais

São os mais variáveis possíveis, contudo iremos abordar três principais tipos de crimes que ocorrem por meio desta rede sendo eles, calúnia, difamação e Injúria, ambos regulados respectivamente pelos artigos 138, 139 e 140 do Código Penal.

Calúnia

O tipo penal da calúnia em seu artigo 138 Caput do Código Penal é definido como:

> **“Calúnia**
> Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime:
> Pena - detenção, de seis meses a dois anos, e multa.”
> (http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm)

Este tipo penal enquadra quem por ventura venha atribuir à vítima algum ato considerado pelo ordenamento jurídico como criminoso, um exemplo fictício dentro do contexto internet seria:

> “Mateus com a finalidade de prejudicar Guilherme, publicou em seu facebook, um texto atribuindo-lhe o roubo que ocorreu na farmácia da vizinhança ”.

Neste exemplo fica claro que Mateus por intermédio de seu facebook, cometeu o crime de calunia a fim de prejudicar Guilherme, ou seja, o meio virtual foi empregado para fazer a publicidade do ato.

Difamação

Aqui conforme o artigo 139 Caput, difamação é definida como:

> **Difamação**
> Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação:
> Pena - detenção, de três meses a um ano, e multa
> (http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm)

Embora se assemelhe muito a calúnia, o tipo penal difamação enquadra quem por ventura venha atribuir a vítima fato que ofenda sua reputação, que não seja necessariamente um fato criminoso, mas como também algo que de alguma forma acabe com sua reputação, um exemplo fictício para tal situação seria:

> “Mateus com intuito de prejudicar o casamento de Guilherme publica em seu facebook comentários dizendo que Guilherme sai com várias mulheres da cidade em que residem”

No exemplo fica claro que Mateus com intuito de prejudicar Guilherme lhe atribui uma qualidade de infiel e da publicidade a isto em sua rede social.

Injúria

Conforme o artigo 140 Caput, do Código Penal injúria é definida como:

> **Injúria**
> Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:
> Pena - detenção, de um a seis meses, ou multa
> (http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm)

Diferente da calúnia e da difamação, o fato criminoso é feito de forma direta a vítima, ou seja, não precisa tornar algo público, porém, pode ser feito através de uma rede social, um exemplo fictício seria:

> "Mateus através do Whatsapp, enviou mensagens a Guilherme lhe ofendendo com palavras de baixo calão e lhe atribuindo características que ofenderam sua dignidade."

O crime é todo praticado por intermédio da rede social, o que antes era todo consumado pessoalmente, hoje é feito sem que as duas partes tenham contato.

2.7.2 – Investigação

Nestes tipos de crimes, a investigação terá início a partir da representação da parte na delegacia da Policia Judiciária, na qual serão apresentados os fatos ao delegado de polícia. O mesmo de posse das informações procedera de acordo com a forma de investigação exposto no item 2.2 deste capitulo.

A vítima poderá ainda, ir até um cartório de notas elaborarem uma ata notarial para provar o alegado, pois nestes casos é comum o autor do crime vir a apagar ou alterar postagens para se eximir dos crimes.

Vale lembrar que as formas de salvar provas exposta por todo item 2.4 deste capitulo são vá lidas, e de suma importância para dar prosseguimento a investigações destes crimes.

2.7.2.1 – Competência da investigação

Em geral a competência nesses crimes, gera certa instabilidade nos tribunais, pois a lei não é categórica em razão da competência nessas situações, diante disto, algumas decisões tendem a se pacificar no que diz respeito ao lugar onde o responsável pelo crime se encontra, conforme um julgado exposto pelo site jus.com.br:

> "Informativo de Jurisprudência Nº: 0434 Período: 10 a 14 de maio de 2010.
> Terceira Seção
> COMPETÊNCIA. INTERNET. CRIMES CONTRA HONRA.
> **A Seção entendeu, lastreada em orientação do STF, que a Lei de Imprensa (Lei n. 5.250/1967) não foi recepcionada pela CF/1988. (...) Quanto aos crimes contra a honra praticados por meio de reportagens veiculadas na Internet, a competência fixa-se em**

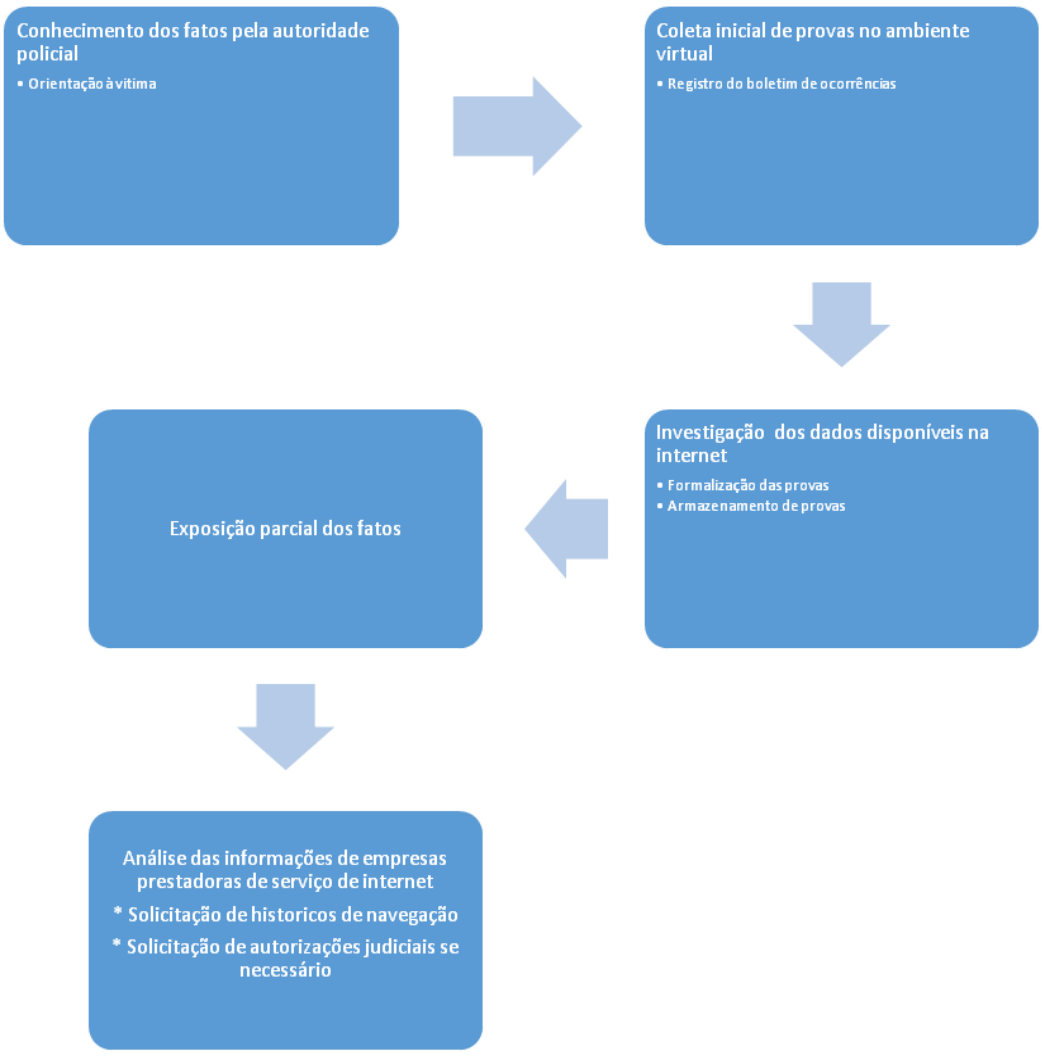
> **razão do local onde foi concluída a ação delituosa, ou seja, onde se encontra o responsável pela veiculação e divulgação das notícias, indiferente a localização do provedor de acesso à rede mundial de computadores ou sua efetiva visualização pelos usuários**. Precedentes citados do STF: ADPF 130-DF , DJe 6/11/2009; do STJ: CC 29.886-SP , DJ 1º/2/2008.CC 106.625-DF, Rel. Min. Arnaldo Esteves Lima, julgado em 12/5/2010."
> (https://jus.com.br/artigos/53229/competencia-para-o-julgamento-de-crimes-contra-a-honra-praticados-na-internet)

Através do julgado podemos considerar que a grande maioria tende a acatar o lugar como aquele em que se encontra o acusado.

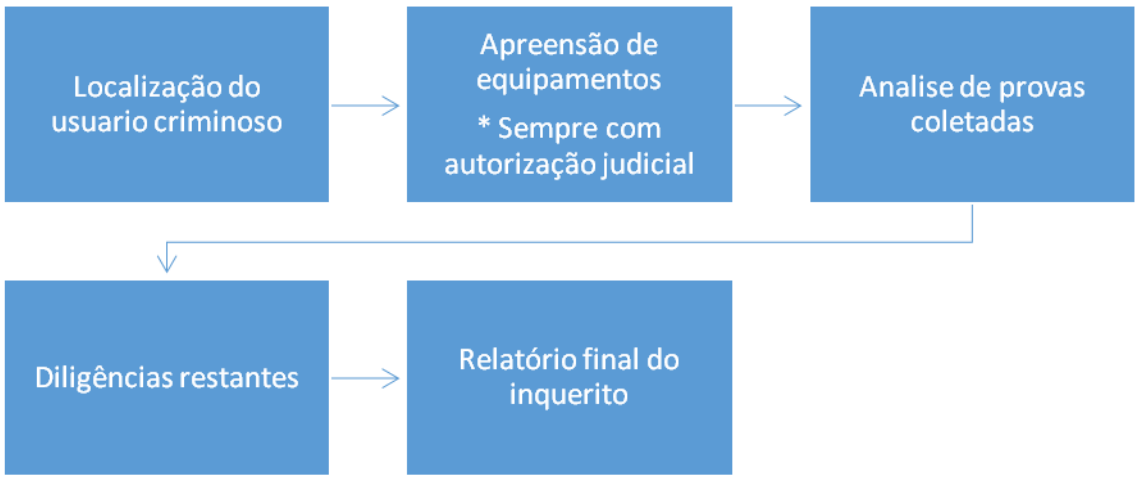
2.8 Procedimento de investigação esquematizado:

Breve esquema das etapas de investigação, citados no capítulo 2.2 desta monografia, de acordo com o exposto na obra de Jorge, Higor Vinicius Nogueira:

Primeira fase



Segunda fase



3. Desafios na investigação

Diante do abordado nos capítulos anteriores, temos uma noção do quanto é vasto a internet e os inúmeros crimes que podem ocorrer dentro dela. Embora nossa polícia

judiciária possua bons métodos de investigação para esses crimes, ainda a muito para evoluir em determinados quesitos as quais serão abordados dentro deste capitulo.

3.1 – Evoluções das tecnologias

A velocidade na qual os meios tecnológicos evoluem atualmente é extremamente acelerada, com isso novos métodos, equipamentos e programas surgem com intuito de serem usados para pratica de crimes. Tal evolução acaba por não ser acompanhada por nosso sistema de investigação, nas palavras de Jorge, Higor Vinicius Nogueira:

> "Nestes termos evolutivos e preocupantes, essas novas formas de praticar crimes representam um grande desafio para os órgãos da persecução penal, que devem ser instrumentalizados para esse enfrentamento. Necessariamente, no Brasil deverá ser traçado um planejamento e uma preparação para todos os problemas penais relacionados com o tema, existentes e os que ainda surgirão."(Jorge, Higor Vinicius Nogueira, 2017, pag. 414)

O Brasil ainda não possui uma linha de planejamento efetiva para acompanhar tais evoluções, acabando por prejudicar as investigações de vários crimes em virtude da falta de instrumentos ou até mesmo pessoas capacitadas para atuar nessas áreas.

3.2 – Impacto na economia

Além da dificuldade em acompanhar as evoluções constantes dos meios tecnológicos, outro problema que acaba por influenciar negativamente no que se refere as investigações, são os prejuízos gerados por esses crimes, conforme Higor Vinicius:

> "Os prejuízos decorrentes dos crimes cibernéticos são de grandes proporções. Segundo a Federação Brasileira de Bancos (Febraban), apesar do investimento na prevenção e no combate a essa modalidade de delito, no ano de 2010 eles provocaram prejuízos de novecentos milhões de reais para as instituições bancárias167. No mundo todo, o prejuízo com as fraudes eletrônicas passa de um trilhão de dólares anual."(Jorge, Higor Vinicius Nogueira,2017, pag. 415).

Esse impacto pode ser ainda maior, pois podemos considerar vários crimes diários que nem ao menos chegam ao conhecimento da polícia, por falta de representação das vítimas desses criminosos. No Brasil esses números também são muito altos, nas palavras Higor Vinicius:

> No Brasil, conforme rotineiras divulgações, o perfil dos criminosos virtuais é voltado principalmente para as fraudes eletrônicas. O prejuízo, conforme divulgado

> pela empresa de antivírus Symantec, chegaria a US$ 114 bilhões170, o que torna o assunto ainda mais preocupante**.** (Jorge, Higor Vinicius Nogueira, 2017, pag. 416)

Os criminosos nessa área no Brasil acabam por faturar até mais que em outras modalidades de crimes cometidos por organizações criminosas.

3.3 – Legislação

Talvez um dos maiores desafios, seja a mudança na legislação brasileira, pois mesmo que vários tipos penais possam a vir ser aplicados em vários crimes virtuais, ainda a casos em que a dúvida surge em relação ao tipo, promovendo assim uma insegurança no meio jurídico. Conforme Higor Vinicius:

> "Cabe esclarecer que é possível realizar o enquadramento típico da maioria das atividades que causem prejuízos ou transtornos aos usuários. Porém, para atender àqueles casos em que não existe a referida previsão penal para promover um enquadramento específico que se amolde perfeitamente aos referidos crimes, de forma a evitar questionamentos jurídicos como, por exemplo, a alegação de que a conduta não é criminosa porque não há previsão legal, e também com o objetivo de oferecer mais condições para a punição dos crimes cibernéticos..." (Jorge, Higor Vinicius Nogueira, 2017, pag. 418)

Embora ainda o legislador tente elaborar leis para inibir esses criminosos, ainda é muito pouco, visto o quão complexo é o tema crimes virtuais, ao meu olhar o que o legislador tem feito apenas é corrigir determinados temas específicos, sem dar uma ênfase maior a esses crimes. Na obra de Higor Vinicius Nogueira ele traz a seguinte informação:

> No dia 16 de maio de 2012, em razão do clamor causado pela divulgação das fotos da atriz Carolina Dieckmann, o plenário da Câmara dos Deputados aprovou o projeto do deputado Paulo Teixeira, que tipifica principalmente o crime de invasão de dispositivo informático. O projeto, PL 2793/2011, foi encaminhado para análise no Senado e, juntamente com a mínima parcela do "projeto Azeredo", foi também aprovado. No dia 30 de novembro de 2012 foi sancionada a Lei 12.737, sendo denominada socialmente e pela mídia de **Lei Carolina Dieckmann.** (Jorge, Higor Vinicius Nogueira, 2017, pag. 421).

Nesta informação fica claro que o legislador somente se atentou a tal tema, em decorrência de uma grande repercussão de um caso especifico que aconteceu, mas, e quanto aos demais anteriores que já ocorram e o nosso legislador acabou por não ser atentar a tal situação, necessitou uma repercussão nacional para que seja formalizada uma lei para regular determinada conduta.

3.3.1 - Marco Civil da Internet

Ao tratar da legislação, não poderia de deixar de abordar o chamado Marco Civil da Internet ou a chamada Lei N° 12.965/14, sancionada em 23 de abril de 2014, teve como objetivo regular alguns aspectos importantes como a Neutralidade na rede, ou seja, o conteúdo que o usuário poderia acessar seria livre, as empresas prestadoras de serviço de internet, não poderiam cobrar mais dependendo do conteúdo acessado.

Privacidade de acesso e a proibição de registro de navegação, nesses dois pontos o Marco Civil da Internet acabou por dificultar e muito a parte de investigação da polícia, nas palavras de Higor Vinicius Nogueira:

> "Existe ainda o projeto do Marco Civil da Internet Brasileira do Ministério da Justiça, que tem causado profunda preocupação em razão de criar obstáculos para a investigação dos crimes em discussão175. Este projeto foi usado para justificar a demora na aprovação da lei de crimes eletrônicos, sob o argumento de que primeiro deveria ser aprovado o Marco Civil no país, para apenas em seguida ocorrer a aprovação da lei que tratava dos crimes cometidos por intermédio de computadores."(Jorge, Higor Vinicius Nogueira,2017, pag. 421).

No que se refere à privacidade de acesso, o site ebc.com.br traz em uma matéria sobre o Marco Civil da Internet:

> O projeto de lei regula o monitoramento, filtro, análise e fiscalização de conteúdo para garantir o direito à privacidade. Somente por meio de ordens judiciais para fins de investigação criminal será possível ter acesso a esses conteúdos. (http://www.ebc.com.br/tecnologia/2014/04/entenda-o-marco-civil-da-internet-ponto-a-ponto)

Com isso o acesso as informações ficou mais restrito, dificultando e atrasando as investigações de crimes cibernéticos, ajudando assim os criminosos a se ocultarem mais facilmente apoiados pela lei.

Ao que se refere à proibição ao registro de acesso, o site ebc.com.br traz na mesma matéria a seguinte informação:

> Segundo o Marco Civil, os provedores de conexão são proibidos de guardar os registros de acesso a aplicações de internet. Ou seja, o seu rastro digital em sites, blogs, fóruns e redes sociais não ficará armazenado pela empresa que fornece o acesso.
> (http://www.ebc.com.br/tecnologia/2014/04/entenda-o-marco-civil-da-internet-ponto-a-ponto)

Todos os vestígios desses criminosos acabam se perdendo em virtude de lei, informações preciosas que serviriam para rastrear e identificar os criminosos,

simplesmente são descartadas com a prerrogativa de proteger a privacidade do usuário convencional, mas que teve seus efeitos benéficos a criminosos especializados em crimes virtuais, sendo mais uma ferramenta para ajudá-los a se ocultar na internet.

3.4 – Necessidade de ordem judicial

Embora a necessidade de ordem judicial surja como um ato para inibir o abuso por parte de autoridades, dentro da investigação de crimes cibernéticos acaba por criar serias barreiras para investigação, nas palavras de Higor Vinicius Nogueira:

> O requisito de ordem judicial para obtenção de toda e qualquer informação relativa a um crime cibernético é outra questão que atravanca a investigação e representa uma das facetas do excesso de burocracia, que apenas prejudica e/ou retarda o esclarecimento desse tipo de delito. A solução ficaria na necessária diferenciação entre os acessos aos dados cadastrais e aos *logs* de conexão e/ou de acesso. (Jorge, Higor Vinicius Nogueira, 2017, pag. 424).

Toda essa burocracia acabar por amarrar a investigação, atrasando a localização do eventual criminoso, aumentando a chances do mesmo se ocultar ou apagar seus vestígios.

3.5 – Capacitação da Polícia

Atualmente dentre todos os desafios da investigação dos crimes virtuais, seja a capacitação dos policias, uma vez que dentro do nosso país ainda temos uma polícia muito defasada em relação a apuração desses tipos de crimes, além da falta de infraestrutura adequada para promover tais investigações. Nas palavras do autor Higor Vinicius Nogueira:

> A falta de capacitação dos policiais e também de outros atores da persecução penal, como o Ministério Público e o Judiciário, representa um grande desafio, na medida em que pode impedir a punição dos *cibercriminosos* e, por consequência, causar impunidade. (Jorge, Higor Vinicius Nogueira, 2017, pag. 425).

Essa falta de capacitação acaba por influenciar negativamente nas investigações, eventualmente atravancando todo o inquérito. Ainda nas palavras do autor, para uma melhora nos resultados das investigações nesses crimes e necessários:

> “A capacitação deve ser realizada continuamente, por profissionais especializados, de modo que os órgãos da persecução possam reprimir e acompanhar a evolução desses crimes. Os integrantes desses órgãos devem ser estimulados por políticas internas a participarem destas capacitações. Ademais, políticas públicas nacionais, voltadas aos órgãos de segurança pública, são bem-vindas e motivarão os estados a investirem na qualificação de seus quadros.”(Jorge, Higor Vinicius Nogueira,2017, pag. 425).

Somente através da qualificação dos agentes, que os resultados irão melhorar, pois, não adianta o estado investir em novos equipamentos, softwares e não capacitar seus funcionários para efetivamente utilizarem todos os novos aparatos fornecidos.

3.6 – Integração entre órgãos de investigação

A comunicação e a troca de conhecimentos entre os órgãos de investigação se faz uma ferramenta muito útil e poderosa nas investigações, mas que, infelizmente dentro do nosso sistema investigativo e deixado de lado muitas vezes, nas palavras do autor Higor Vinicius Nogueira:

> É considerada voz uníssona entre os órgãos que promovem a investigação de crimes praticados pela internet que, diferentemente dos criminosos, não existe uma atuação integrada entre os responsáveis pela persecução penal, mesmo aqueles pertencentes ao mesmo setor.

O que deveria funcionar em constante consonância, acaba por agirem de forma isolada, até mesmo dentro de seus próprios setores. Outro ponto que vale destacar é que o Brasil ainda possui números muito baixos em relação às delegacias especializadas, conforme cita o autor Higor Vinicius Nogueira:

> “O próprio Brasil, em termos de polícias judiciárias estaduais, possui menos de cinquenta por cento de seus Estados com órgãos especializados. Dispõem de Delegacias de Polícia Especializadas apenas Rio de Janeiro, São Paulo, Minas Gerais, Pará, Rio Grande do Sul, Paraná, Espírito Santo, Sergipe, Piauí e Bahia. Outros dois Estados, Distrito Federal e Mato Grosso, possuem órgãos que oferecem orientações aos demais sobre como proceder as investigações. (Jorge, Higor Vinicius Nogueira,2017, pag. 426).

O Brasil ainda tem um caminho muito longo, para enfrentar de forma efetiva os crimes virtuais, seja a especialização de seus agentes, modernização de seus sistemas e integração nacional.

3.7 – Cooperação Internacional

A internet por se tratar de algo tão vasto e global, se faz necessária a cooperação internacional, uma vez que os cibercriminosos podem em agir em qualquer parte do globo, somente de frente do seu computador. Conforme o autor Higor Vinicius Nogueira:

> No ano de 2001, na Hungria, foi criada a Convenção de Budapeste, também conhecida como Convenção sobre o Cibercrime, pelo Conselho da Europa. Dentre suas principais finalidades cabe destacar: o incremento para a cooperação internacional entre os órgãos responsáveis pela investigação criminal; a previsão de novas condutas criminais que, pela internet, causem prejuízo ou transtorno para a vítima; a pressão para aprovação de legislação específica sobre o tema etc.(Jorge, Higor Vinicius Nogueira,2017, pag. 426)

Isto demonstra que os crimes virtuais estão a cada ano que passa tomando proporções ainda maiores e com reflexos na economia de vários países pelo globo, conforme ainda o autor:

> O Brasil deve se tornar signatário do referido tratado ou sugerir sua modificação, pois a tendência é que continuem aumentando os casos nos quais criminosos ou informações que permitam esclarecer a autoria do crime estejam no exterior, de modo que a cooperação internacional é imprescindível para a busca da verdade, ou seja, para que se atinja o absoluto esclarecimento sobre o crime em apuração e suas circunstâncias. (Jorge, Higor Vinicius Nogueira, 2017, pag. 427)

O Brasil por estar atualmente entre os países que mais acessam a internet se vê na necessidade de criar parcerias internacionais a fim de combater esses criminosos no ambiente virtual.

3.8–Interpol no Brasil

A I**nterpol (Inter**national Criminal **Pol**ice Organization), talvez seja um dos órgãos mais famosos no mundo em relação a investigações criminais e tem como finalidade a cooperação entre as polícias de vários países.

No Brasil conforme o site Wikipédia:

> A Polícia Federal é a representante brasileira da INTERPOL. O escritório da Interpol no Brasil localiza-se no complexo da Polícia Federal em Brasília, com representações estaduais em todas as Superintendências Regionais da PF. Sua função é promover a cooperação com organizações policiais de outros países, em estrita coordenação com a Sede da Interpol, em Lyon (França). Policiais Federais da Interpol trabalham na tradução e divulgação de informação criminal internacional, cooperação em investigações internacionais, repressão de crime transnacional, e a busca de foragidos da Polícia de outros países que se encontrem no Brasil.*(https://pt.wikipedia.org/wiki/Interpol)*

Vale lembrar que nos crimes virtuais a cooperação internacional se tornou algo de suma importância, pois os criminosos podem agir de vários lugares do mundo sem ter que tocar o solo do país em que cometeu o crime, apenas se utilizando da internet de onde estiver.

3.9 - **Conscientização dos usuários de internet**

Por fim talvez a arma mais importante, seja a conscientização da população sobre o uso seguro da internet e eventualmente os riscos escondidos dentro dela, pois, conforme o autor Higor Vinicius Nogueira:

> Grosso modo, pode-se dizer que os usuários de internet não conhecem a dimensão dos riscos que a utilização da rede mundial de computadores proporciona, nem as ameaças que enfrenta ao receber um e-mail, acessar um site ou instalar um programa em seu computador. (Jorge, Higor Vinicius Nogueira, 2017, pag. 427).

O usuário convencional, é o elo mais fraco desta corrente, cabe direcionar a ele essa educação e conscientização digital, de acordo com Higor Vinicius Nogueira:

> Esse processo de aprendizado e conscientização, ou seja, de educação digital, parte não só dos órgãos de prevenção, mas também de repressão. A partir do momento em que os policiais informam os usuários sobre como ocorre, por exemplo, determinada fraude, há possibilidade de o usuário se precaver e não ser mais uma vítima de crimes cibernéticos.

Talvez esse seja o processo mais demorado e complexo de ser enfrentado por parte da investigação, mas com as devidas medidas a serem tomadas, uma efetiva campanha de conscientização e instrução dos usuários, com toda certeza que os crimes virtuais em sua grande maioria irão gradativamente diminuir e com isso tornando o ambiente virtual mais seguro.

4 **CONCLUSÃO**

Os crimes virtuais, eventualmente se tornarão cada vez mais comuns em nosso cotidiano, sendo assim nosso sistema jurídico deve ser aprimorado cada vez mais, sempre caminhando junto com as novas tendências e inovações tecnológicas disponíveis.

Infelizmente no atual cenário brasileiro, estamos engatinhando a respeito de investigações de crimes virtuais, embora exista todo um método de investigação a qual foi discorrido neste trabalho, falta delegacias devidamente equipadas e preparadas, agentes públicos devidamente treinados e qualificados para atuarem nesses crimes, além de um novo sistema de normas que possam facilitar os meios de investigação e não criar obstáculos que torne a investigação destes tipos de crimes ainda mais demorado.

Claro que tudo isso deve ser somado a uma boa tática de prevenção desses crimes, atuando na educação digital da população brasileira, instruindo os meios corretos de se proteger no ambiente virtual, para que assim possamos diminuir e muito o número de vítimas e amenizar os prejuízos causados por esses crimes.

5. REFERÊNCIAS

Emerson Wendt e Higor Vinicius Nogueira Jorge**. Crimes Ciberneticos: Ameaças e Procedimentos de Investigação**. 2ª Edição, 2017, Editora Brasport,;

Fernando Capez. **Curso de Processo Penal**. São Paulo, 2016, 23º Edição – Editora Saraiva;

https://g1.globo.com/economia/noticia/mais-de-63-dos-domicilios-tem-acesso-a-internet-aponta-ibge.ghtml

http://www.ebc.com.br/tecnologia/2014/04/entenda-o-marco-civil-da-internet-ponto-a-ponto

https://www.tecmundo.com.br/seguranca/32327-76-dos-usuarios-brasileiros-ja-cairam-em-golpes-virtuais.htm

https://cgi.br/historicos/#1995

http://revistapesquisa.fapesp.br/2011/02/18/prim%C3%B3rdios-da-rede_/

https://pt.wikipedia.org/wiki/Backbone

https://pt.wikipedia.org/wiki/ARPANET

https://tecnoblog.net/56910/eniac-primeiro-computador-do-mundo-completa-65-anos/

https://pt.wikipedia.org/wiki/Interpol