FACULDADE DE CUIABÁ
CURSO DE DIREITO

ALAN SOARES DE OLIVEIRA

CRIMES CIBERNÉTICO E OS DANOS CAUSADOS NO BRASIL

Cuiabá/MT
2022/1

ALAN SOARES DE OLIVEIRA

CRIMES CIBERNÉTICO E OS DANOS CAUSADOS NO BRASIL

Trabalho de Conclusão de Curso apresentado à Banca Avaliadora do Departamento de Direito, da Faculdade de Cuiabá - FASIPE, como requisito parcial para a obtenção do título de Bacharel em Direito.

Orientador: Profº: Sonny Taborelli

Cuiabá/MT
2022/2

ALAN SOARES DE OLIVEIRA

CRIMES CIBERNÉTICO E OS DANOS CAUSADOS NO BRASIL

Trabalho de Conclusão de Curso apresentado à Banca Avaliadora do Curso de Direito - FASIPE, Faculdade de Cuiabá como requisito parcial para a obtenção do título de Bacharel em Direio.

Aprovado em ____/____/____

Sonny Taborelli
Professor(a) Orientador(a) Departamento de Direito -FASIPE CPA

Luana Fatima Zapello
Professor(a) Avaliador(a) Departamento de Direito -FASIPE CPA

Diego Castro de Melo
Professor(a) Avaliador(a) Departamento de Direito – FASIPE CPA

Ronildo Medeiros Junior
Coordenador do Curso de Direito FASIPE CPA - Faculdade de Cuiabá

Cuiabá/MT
2022/2

DEDICATÓRIA

A todas as pessoas que em minha caminhada demonstraram paciência e carinho.
Em especial, àquelas que me incentivaram a seguir sempre em frente.

AGRADECIMENTO

- Acima de tudo a Deus, porque se não fosse através dele, não teria chegado até aqui.
- Aos meus pais, que me ajudaram a dar os primeiros passos na vida.
- Ao professor orientador, que me orientou de forma objetiva para obter êxito neste trabalho.
- Aos demais professores, do curso degraduação, que nos transmitiram seus conhecimentos e muito contribuíram para nossa formação.
- A empresa onde foi realizado o estágio, pela ajuda e disponibilidade de seus colaboradores.
- A todos que direta e indiretamente contribuíram para a realização deste trabalho e permitiram o enriquecimento de minhaaprendizagem.

EPÍGRAFE

Regozijar-me-ei muito no SENHOR, a minha alma se alegrará no meu Deus; porque me vestiu de roupas de salvação, cobriu-me com o manto de justiça, como um noivo se adorna com turbante sacerdotal, e como a noiva que se enfeita com as suas jóias.
Isaías 61:10

OLIVEIRA: Alan Soares. **CRIMES CIBERNÉTICO E OS DANOS CAUSADOS NO BRASIL.** 2022. 38. Monografia de Conclusão de Curso – FASIPE – Faculdade de Cuiabá.

RESUMO

Ao longo da evolução do ser humano se deparamos com a internet, que nos trouxe muitos avanços, fez com que o mundo ficasse de alguma forma acessível a todos pois, consegue pesquisar sobre tudo em segundos e também se comunicar com pessoas do outro lado do mundo em tempo real foi uma evolução gigantesca para toda a sociedade com isso vemos que pessoas se aproveita dessa falta de conhecimento do que é novo e usam para praticar crimes de diversas amplitudes os famosos (crimes cibernéticos) são aqueles que utilizam de computadores e dispositivos eletrônicos para praticar ações criminosas, que geram danos a indivíduos ou a patrimônios, visando extorsões de recursos financeiros e danos a reputação vítimas na internet com isso vamos verificar os danos causados pôr os crimes cibernéticos sendo eles danos psicológicos envolvendo bullying, racismo, fake news, roubo de dados pessoais, por tais razões este trabalho irá contar com os objetivos de desmistificar o tema abordado e os especificos se encontram em compreender o conceito de crimes cibernéticos, crimes puros e impuros bem como a analise jurídica do tema proposto, para que todo o trabalho seja devidamente guiado, foi proposto a seguinte problemática o crime cibernético ainda é um problema no Brasil?, para que essa pergunta seja solucinada é que o trabalho passa a demonstrar sobre o desenrolar dos preceitos dos crimes cibernéticos.

Palavras chave: Segurança de Danos; Crimes cibernéticos; Lei de Proteção de Dados.

OLIVEIRA: Alan Soares. **CYBER CRIME AND THE DAMAGES CAUSED IN BRAZIL.** 2022. 38. Monografia de Conclusão de Curso – FASIPE – Faculdade de Cuiabá.

ABSTRCT

Throughout the evolution of the human being, we have come across the internet, which has brought us many advances, has made the world somehow accessible to everyone, because it can search about everything in seconds and also communicate with people on the other side of the world. in real time was a gigantic evolution for the whole society with that we see that people take advantage of this lack of knowledge of what is new and use it to commit crimes of different amplitudes the famous (cyber crimes) are those who use computers and electronic devices to practice criminal actions, which generate damage to individuals or property, aiming at extortion of financial resources and damage to the reputation of victims on the internet. personal data, for these reasons, this work will have the objective of demystifying the topic addressed and the specific ones involved. In order to understand the concept of cyber crimes, pure and impure crimes, as well as the legal analysis of the proposed theme, so that all the work is properly guided, the following problem was proposed is cyber crime still a problem in Brazil?, so that this question to be solved is that the work goes on to demonstrate about the unfolding of the precepts of cyber crimes.

Keywords: Damage Safety; Cyber crimes; Data Protection Act.

Sumário

INTRODUÇÃO

Ao longo da evolução do ser humano, se depara com a internet, que nos trouxe muitos avanços, fez com que o mundo ficasse de alguma forma acessível a todos pois, consegue pesquisar sobre tudo em segundos e também se comunicar com pessoas do outro lado do mundo em tempo real foi uma evolução gigantesca para toda a sociedade com isso vemos que pessoas se aproveita dessa falta de conhecimento do que é novo e usam para praticar crimes de diversas amplitudes os famosos (crimes cibernéticos), são aqueles que utilizam de computadores e dispositivos eletrônicos para praticar ações criminosas, que geram danos a indivíduos ou a patrimônios, visando extorsões de recursos financeiros e danos a reputação vítimas na internet com isso vamos verificar os danos causados pôr os crimes cibernéticos sendo eles danos psicológicos envolvendo *bullying*, racismo, *fake news*, roubo de dados pessoais.

Danos materiais como golpes da olx, sequestro de dados de empresa, leilões falsos, entre outros. na prática é observado muita impunidade por parte dos criminosos pois a maiorias dos golpes nem denunciados são ou por falta de informação ou por vergonha de denunciar nos casos psicológicos.

Tocar nesse assunto é importante pois as maneiras de se evitar e saber como são feitos, a maioria das pessoas por acham que a internet é um mundo sem impunidade acabam deixando com que pessoas que praticam vários crimes fiquem impunes.

1. CONCEITO HISTÓRICO SOBRE CRIMINALIDADE CIBERNÉTICA

Para iniciarmos o trabalho de forma objetiva, tudo se inicia com a história da internet e suas evoluções perante o tempo, bem como a análise sobre o uso da internet e onde foi o marco para que o crime cibernético tomasse tamanha proporção, o qual sabe-se que a internet em tempos atuais é uma ferramenta indispensavel para o dia a dia de grande parte da população.

Pensando nisso MILAGRES (2016) declara que "os crimes cibernéticos são uma extenção dos crimes proprimanete ditos", logo, para que toda a contextualização do tema definitivamente abordado, desta forma para melhor compreender será dividido em subtópicos, tais como a distinção do crime cibernético puro e impuro, crimes contra a honra entre outros que poderão ser visto no decorrer deste trabalho.

A internet antes mesmo de ser usada como ferramenta para o crime, foi muito utilizada para a evolução dos tempos modernos, podendo se vender, propagar, comprar entre outras ferramentas possiveis através da internet, logo destaca novamente MILAGRES (2016) "A Internet é um avanço dos tempos modernos, ferramente está que serve para uma gama milenar para serviços e outros".

Portanto os crimes cibernéticos com o advento dos boicotes ao sistemas de tecnologias que utilizavam da internet para seu funcionamento (MILAGRES 2016). Um ponto histórico a ser lembrado é o exemplo do boicote com a empresa Jacquard, onde sabotaram o funcionamento mecanico da sua empresa o prejudicando de forma crucial para o desempenho grandioso da empresa em questão.

Em outro periodo, ja no ano de 1978 alguns estudantes de uma universidade, entraram no sistema da escola e fizeram alterações no sistema de notas, através da utilização da internet. (MILAGRES 2016). Pensando nisso, é que advem a termologia do crime cibernético, não se trata de um crime propriamente dito de inicio, mas sim do crime de boicote com o sistema

alheio.

Pensando no desenvolvimento da sociedade e suas intenções com a internet, o STJ divulga o conceito basilar de crime na internet e algumas classificações, vejamos:

> **A 3ª Seção do STJ firmou entendimento no sentido de que a subtração de valores de conta-corrente mediante transferência eletrônica fraudulenta configura crime de furto, previsto no artigo 155**, parágrafo 4º, inciso II, do Código Penal.
> Uma discussão frequente em processos que chegam à corte diz respeito ao juízo competente para analisar os casos em que o furto acontece via rede mundial de computadores. Nesses casos, para o STJ, a competência é definida pelo local onde o bem foi subtraído da vítima.
> Ao apreciar conflito de competência (CC 145.576) em processo que envolveu furto mediante transferência eletrônica fraudulenta de contas-correntes situadas em agência bancária de Barueri (SP) – mesmo tendo os valores sido enviados para Imperatriz (MA)
> (BRASIL STJ 2015).

A transferencia entre contas correntes mediante fraude se torna uma tipologia conceitual de crime cibernético, ficando claro esse primeiro conceito do SJT. Em visão jurisprudencial após a está, o STJ declara que:

> **Criar sites na internet para vender mercadorias com a intenção de nunca entregá-las é conduta que se amolda ao crime contra a economia** popular, previsto no artigo 2º, inciso IX, da Lei 1.521/51, como definiu a corte (CC 133.534).
> Segundo a decisão, ao criar um site para vender produtos fictícios pela internet, os criminosos não têm por objetivo enganar vítimas determinadas, mas, sim, um número indeterminado de pessoas, vendendo para qualquer um que acesse o site.
> (BRASIL STJ 2015).

Entende-se que a criação de sites fraudulentos e com a devida intenção de não entregar o produto oferecido, se torna crime cibernético, devido alguns requisitos que vimos acima, desta feita estabelecendo outro conceito caracteristico do crime.

Por fim, o crime de ameaça em conjunto com o crime cibernético, tendo como essencia o crime pela internet haja visto seu genero de fato, vejamos o entendimento do STJ sobre a ameaça pelo WahtsApp:

> Nas hipóteses de ameaças feitas por redes sociais como o Facebook e aplicativos como o WhatsApp, o STJ tem decidido que o juízo competente para julgamento de pedido de medidas protetivas será aquele de onde a vítima tomou conhecimento das intimidações, por ser

> este o local de consumação do crime previsto no artigo 147 do Código Penal.
> Com base nesse entendimento, a 3ª Seção fixou a competência da comarca de Naviraí (MS) para a análise de pedido de concessão de medidas protetivas em favor de mulher que teria recebido pelo WhatsApp e Facebook mensagens de texto com ameaças de pessoa residente em Curitiba (CC 156.284).
> (BRASIL STJ 2015).

Deve-se saber que os crimes informáticos são tratados como crimes criptograficos, ou seja, para pessoas que detem o conheicmento da criptografia e fazem dela a arte de burlar o sistema através de outro sistema invasor, passando por barreiras de segurança com facilidade entre outros (SILVA, 2016).

A cripitografia se conceitua como a arte de mascarar, esconder, desvirtuar a realidade das informações através de uma informação criptografada, a pratica é antiga porém muito pouco estudada, por isso da relevancia do estudo aprofundado sobre o sistema de informações sobre o tema proposto.

Portanto, o avanço da criptografia é uma inovação tecnológico que deve ser elucidado, pois passou por evoluções significativas e apartir da criptografia é que a internet teve avanços e como funciona de maneira singular. Desta forma, a criptografia é a ciência da informação ou da ocultação de informação, e considerada a primeira forma rudimentar de comunicação, muito utilizada em guerras em tempos passados. (SILVA, 2016).

Um dos eventos mais conhecido foi na Segunda Guerra mundial, onde o pai da computação, conhecido também por Alan Turing, foi um excelente matemático e britânico que na gerra prestou seus serviços para a inteligência do pais, o qual foi responsavel por criar tecnicar de quebra de segurança dos códigos alemães, desta feita na epoca foi reconhecido como maior cripitófogo e aperfeiçoou a técnica cada vez mais. (SCHECHTER, 2016)

Carvalho (2006) explica que no avanço das guerras, o reconhecimento do armamento é algo muito bom porém o avan ço na proteção do sistema é algo imprescindivel, pois muito dos pontos de ataques se iniciam através de comandos criptografados entre sistemas interligado a radio ou internet. Nesse contexto a internet começou a obter uma grande notoriedade entre os avanços dos crimes informaticos, pois se partia de um preceito doloso de prejudicar pessoas. (CARVALHO 2006)

A internet toma alguns avanços ao público, ou seja, um grande avanço para o mundo, no entanto, com altos riscos a ser enfrentados, portanto, somente no ano de 1988 nos Estados Unidos, onde foram iniciado a venda de internet comom forma de comercio (PAESANI 2000).

Na nos anos seguintes, inicia-se a grande revolução tecnológica em respeito a internet e equipamentos que se utilizavam da mesma, logo, a mudança entre paises e da propria população se tornou algo de cunho mundial, pois a corrida de quem tinha a tecnologia mais avançada se tornava o rumo dos paises visinhos e dos criadores e aproveitadores da internet. (CARVALHO 2006)

Cibercrime se inicia em uma vase mais virtual, pois se trata de critografias que buscam proteger dados corporativos, então a meta dos criminosos que se utilizavam do conhecimento da criptografia se tornou o objetivo maior dos criminosos, o qual busca quebrar o maximo de sigilos e dados pessoais, bancarias entre outros (CARVALHO 2006).

1.1 CRIMINALIDADE CIBERNÉTICA

Partindo para um conceito mais formal sobre o crime cibernético passa-se a expor um pouco mais sobre o crime propriamente dito. Assim D´URSO (2017) explana que “no virar do milenio, o mundo digital se torna uma ferramente extremamente fascinante”, desta forma com a popularizaçlão da internet e seu uso amplamente divulgado e comercializado, abre-se uma janela sobre o uso obscuro da internet. (D´URSO 2017).

Haja vista o nome cibercrime esteja defasado, criou-se essa pronuncia para indentificar os criminosos da decada de 90, os quais utilizavam da internet para cometer alguns crimes possiveis através da criptografia, muito visto em guerras. Porem, na reunião do G-8, discutil-se a utilização da internet de forma desinfreada mas que surgisse leis que pudesse haver para limitações do uso (D’URSO, 2017).

A progressividade da evolução tecnologica e a mutanção da internet e seus apetrechos, fazem com que os crimes ciberneticos diminuam, no entanto, levando em consideração que a evolução deve ser constante, pois com o uso da internet sendo usada de formato livre, alguns criminosos se aperfeiçoam com estudos e aprimorações com a quebra dos dados da internet, pois o conhecimento é vasto em relação a criptografias e internet de uso geral (MILAGRES 2016).

No entendimento de MILAGRES (2016), os criminoso que invadiam os dados e roubavam ou burlavam algumas seguranças, eram denominados de “HACKERS”, o nome apesar de moderno, esses individuos ja eram conhecidos desde as primicias da internet, o qual tinha como base a criptografia e a quebra do sigilo realizada por essas pessoas.

A termologia hacker veio da lingua inglesa, o qual tem o conceito de programadores

habilidosos e possuidores de conhecimento avançado referente a internet, essas pessoas eram capazes de descobrir e coletar dados de modo sorrateiro, sem que sejam pegos ou identificados, podendo se aproveitar disto para trocar, alterar ou desvirtuar informações realistas por falsas (TOLEDO, 2017).

Com o avanço da tecnologia, os estelionatários veem esse apetrecho como uma saida ou uma inovação no meio dos golpes, as transações comerciais eram os que mais chamavam atenção, por isto, as movimentações bancarias eram muito cuidadoso o seu procedimentno, no entanto, nem tudo estava seguro, pois o aperfeiçoamento de roubos através dessa ferramente dava inicio a uma nova era de furtos. (TOLEDO, 2017).

Um dos mecanismos mais utilizados pelos estelionatarios nas paginas de internet, com o cunho de promover alguma venda, ou realizar emprestimos pessoais dentre outros, se aproveitavam da inocencia de algumas pessoas, e pegavam dados importantes para a realização do estelionato. (TOLEDO, 2017).

No artigo 184 do Código Penal, o qual dispõe:

> Art. 184. Violar direitos de autor e os que lhe são conexos: (...) § 3o Se a violação consistir no oferecimento ao público, mediante cabo, fibra ótica, satélite, ondas ou qualquer outro sistema que permita ao usuário realizar a seleção da obra ou produção para recebê-la em um tempo e lugar previamente determinados por quem formula a demanda, com intuito de lucro, direto ou indireto, sem autorização expressa, conforme o caso, do autor, do artista intérprete ou executante, do produtor de fonograma, ou de quem os represente.(BRASIL. CP 1940)

Veja-se que o parágrafo 3º do artigo mencionado, discorre sobre a violação por meio da internet, assim, classificando o crime cibernetico através de outro delito, tendo como exemplo o estelionato. Sendo importante destacar que no artigo o crime de informação seria o crime de violação dos direitos autorais, sendo o paragrafo dito acima ramificando o crime tipificado, entrando assim como majoração de pena, ou conhecida como qualificadora. (TOLEDO, 2017).

Desta maneira, todo crime ou conduta delituosa que ocorra de maneira online, sendo ela o tráfico, prostituição, sabotagem, terrorismo e outros, entram como crimes cibernéticos, sendo a sua majorante. Esses tipos de crimes ocorrem em todo o mundo, principalmente no Brasil, o qual causa transtornos e deixa uma onda crescente deste tipo de crime (MILAGRES 2016).

O informativo 335 da MP/PR discorre que:

> Crimes na Internet - Competência
> 12/06/2015
> Com o crescimento da utilização de computadores e do uso da internet, a criminalidade informática elevou os índices de pessoas vítimas de fraudes, crimes contra a honra, racismo, a propagação da pornografia infantil, dentre outros delitos.
> É notória a mudança social abarcada pela globalização da internet que trouxe nova forma de comunicação e modificou as relações sociais em todo o mundo, contudo, junto com tais benefícios surgiram também novos riscos, impondo a necessidade do controle jurídico. O dinamismo e versatilidade, inerentes à internet, tornaram-se foco de preocupação para o poder legislativo que editou as Leis 12.735/12, 12.737/12 (Lei Carolina Dieckman – altera os art. 154, 266 e 298 do CP) e 12.965/14 (Marco Civil da Internet).

Em seguida dispõe a jurisprudência correlatada ao informativo:

> CONFLITO NEGATIVO DE COMPETÊNCIA. PROCESSUAL PENAL. APURAÇÃO DO DELITO DO ART. 241-A DO ESTATUTO DA CRIANÇA E DO ADOLESCENTE. SUPOSTA VEICULAÇÃO DE IMAGENS DE PORNOGRAFIA INFANTIL PELA INTERNET. COMPETÊNCIA FIRMADA PELO LUGAR DA INFRAÇÃO. ART. 70 DO CÓDIGO DE PROCESSO PENAL. COMPETÊNCIA DE TERCEIRO JUÍZO, ESTRANHO AO CONFLITO. 1. A consumação do delito, que atualmente tem previsão no art. 241-A do Estatuto da Criança e do Adolescente, "ocorre no ato de publicação das imagens pedófilo-pornográficas, sendo indiferente a localização do provedor de acesso à rede mundial de computadores onde tais imagens encontram-se armazenadas, ou a sua efetiva visualização pelos usuários" (CC 29.886/SP, Rel. Ministra MARIA THEREZA DE ASSIS MOURA, TERCEIRA SEÇÃO, julgado em 12/12/2007, DJ 01/02/2008, p. 427).

Um caso muito repentino aconteceu com um Hospital do Cãncer em barretos, onde se valia do dinheiro virtual para suas transações, compras de remédios, pagamentos de funcionarios e outros, bem como o sistema de dados dos pacientes, foram perdidos, os lançamentos via internet foram apagados e causou um transtorno enorme para o hospital, em contra partida, os sequestradores de dados pediram depositos em moedas virtuais com dificil rastreio, para que voltasse o sistema ao normal, não feito a transação o hospital passou três dias trabalhando de forma manual, atrasando atendimentos (TOLEDO, 2017).

1.2 PRINCIPAIS AMEAÇAS

Neste tópico será observado sobre as ameaças no sentindo principal em relação aos computadores e seus mecanismos. Desta feita todo o cuidado com que se acessa pelo computador, bem como, aceitar alguns termos sem ler, fazem com que esse tópico seja relevante para o desenvolvimento do tema tratado no presente trabalho.

Abrindo o tópico descrito, os computadores apresentam uma divercidade muito grande em relação aos seus disposiutivos e dispositivos bvaixados direto pela internet, e por isso por se tratar de crimes praticvados pela internet, o sistema de segurança é um mpetodo de defesa que deve sempre estar atualizado com as gerações atualizadas de sistemas de burlar mecanismos operacionais.

Ter o conhecimento sobre os dispositivos maliciosos faz com que diminua a probabilidade de cair em golpes encontrados em sites e outros dispositivos do computador. A preocupação com o conhecimento sobre o tema se destaca não somente para o trabalho academico apresentado, mas sim, para todo o ambito leggislativo, judiciário e investigativo.

No entendimento de TAMEGA (2003). “Os virus é um mecanismo programático que faz parte de alguns programas dos computadores baixados pela internet”. Desta forma possibilitando a cópia dos programas e dados dos computadores que foram infectado por este virus.

QUEIROZ explica que:

> […] Um delito típico de internet seria quando uma pessoa se utiliza de um computador acessando a rede, invade outro computador e obtém, destrói, ou altera um arquivo pertencente ao sistema, ainda que não havendo qualquer obtenção de vantagem patrimonial, mas tão somente a obtenção, destruição ou alteração de dados daquele sistema restrito – circunstância esta que já caracterizaria o tipo penal específico (QUEIROZ, 2008, p.174)

A infecção pelo virus é algo tão simples de ser evitado, tal como verificar o pendrive em sistema de segurança instalado no computador, caso este esteja com virus o programa irá detectar e recomendar a formatação geral do pendrive, para evitar maiores problemas com virus que possa clonar ou enviar dados para outro receptor.

Para QUEIROZ (2008) dispõe em seu entendimento que um dos mecanismo de interferrência via internet com o intuíto de burlar ou colher dados de forma fraudulenta é o sistema que possui a nomenclatura “BOTNET”, os cuidados com esse tipo de programa deve

ser redobrada, pois nasci aqui um programa fraudulento ou copiador.

Esse tipo de programa tem um mecanismo muito complicado, ele conduz o computador a abrir varias guias de internet de forma distributiva causando sobrecarga no computador, ao reiniciar o computador ou até mesmo desligar e ligar pelo cabo de carga, o aplicativo finaliza a instalação e compartilhamento de seus dados (QUEIROZ 2008).

BARRETO explica que:

> A problemática que ora se apresenta é a seguinte: são mais de 117 milhões de usuários de internet no Brasil, alcançando 57,6% de penetração na população, com um crescimento de 2.253,1% no período compreendido entre os anos 2000 e 2015, havendo uma tentativa de fraude a cada 16,6 segundos no país, de acordo com o indicador Serasa Experian de maio de 2015. Como fica então a regulamentação legal no Brasil das relações no ambiente virtual?. (Barreto, 2016. p. 06)

As ameaças são crescente, logo, sempre deve ser observado as atualizações dos programadores e programas de defesa no computador. A transmissão ou a indentificação de um virús se torna vital para a durabilidade do computador e de maiores transtornos com a possibilidade de dados pessoais até mesmo contas bancáriuas sejam divulgado de forma indevida.

Ja na visão de FERREIRA (2015), este relata que, a *defacement* é um mecanismo utilizado por hakers e pessoas com má intençlão. Pois esse tipo de programa ou conhecido como ameaça pichada na internet, são caracterizados pelos ataques políticos, ambientais e religiosas bem como outras possiveis de divulgação na internet de cunho maior de abrangência.

Outra ameaça de virus muito conhecido no mundo virtual e por pessoas mais leigas no assunto é o famoso CAVALO DE TRÓIA, esse virus é advindo de alguma instalação aparentimente sem risco algum, no entanto ele vem por trás ou escondido na instalação e ataca de forma sorrateira, não levantando maiores alertas em referência a detecção do problema.

A maior caracteristica de infecção por esse virus é quando a pessoa recebe algum código malícioso e abre uma porta dos fundos o qual possibilita a entrada do virus ao sistema operacional do computador. É considerado como grave ameaça ao computador, pois esse tipo de virus toma t otal controle da maquina (TAMEGA 2003).

Existe uma tipologia nova de virus, o qual é denomidada de Keylogger, NASCIMENTO discorre sobre:

> Keylogger é um programa criado para gravar tudo o que uma pessoa

> digita em um determinado teclado de um computador. Ele é um programa do tipo spyware e é utilizado quase sempre para capturar senhas, dados bancários, informações sobre cartões de crédito e outros tipos de dados pessoais. Ataques de phishing muitas vezes utilizam keyloggers, que são instalados indevidamente nos computadores das vítimas, para conseguirem obter acesso a dados pessoais com finalidade fraudulenta. (NASCIMENTO Pg 25 2014).

Como pode se observar, esse virus é complexo e muito bem elaborado, pois ele copia tudo aquilo que vc digita em seu teclado, ou seja se voce tem acesso ao banco pelo computador, acaba digitando a senha através do teclado e sendo repassado para outra pessoa, sem ocntar os demais acessos possiveis no computador.

Todo o cuidado com os virus acabam sendo maiores advindo do aprofundamento maior sobre a questão levantada, por isso merece destaque, pois não se trata apenas de copiar o que a pessoa está digitando mas é possivel também tirar foto da tela de onde se está acessando, o que torna o crime mais fácilo do que ja é praticamente.

Em uma reunião com membros do STJ, Martins (2021) declarou que:

> Os criminosos, percebendo o uso mais intenso da internet por grande parte da população mundial, procuraram se adaptar rapidamente à nova realidade, para cometer fraudes eletrônicas. "Cabe ao Estado brasileiro aprimorar seu arcabouço normativo para impedir que esses crimes sejam praticados, evitando prejuízos financeiros e patrimoniais às pessoas, às empresas e ao próprio poder público". (MARTINS pg 02 2021).

Vimos que, apesar da melhoria e dos aperfeiçoamentos gerados até hoje para que se evite tal crime, este ainda é praticado de maneira grandiosa, fazendo comn que o presente tema seja estudado com mais afinidade sobre os virus e suas implicações no cotidiano e as práticas ilicitas dos hakers em relação a atos maliciosos na internet.

Outro mecanismo muito praticado, considerado como ameaça de grande relevância, é o tipo *Hikacker*, esse tipo de virus toma conta de seu nevegador e lhe direciona para outras paginas totalmente malicoisas, onde os botões de sair as vezes são maquiados com aceitar e outros tipos como baixar arquivo entre outros. (duarte 2015).

. Outro meio de ameaça na internet se chama *Rootkits*, esse tipo de vírus faz com que seu computador seja espelhado ou liberado remotamente para o computador do invasor, ou seja é um espelho totalmente funcional do computador invadido para o computador invasor, dessa maneira todos os arquivos guardados acessos entre outros, ficam visíveis para quem está do outro lado da tela.

O problema maior desse tipo de vírus, é que ele se torna invisível por grande parte dos antivírus, ou seja, os antivírus tradicionais acabam não capitando a invasão e acabam ficando infectados por um grande período até descobrir que foram praticante clonado.

Em outro momento, esclarecer que outro mecanismo de fraude na internet que merece atenção, é o *SNiffers*, nesse momento é um dos mais usados, pois esse programa fraudulento monitora todos os acessos a internet, analisando dados de tráfegos entre outros.

Esse programa pode fornecer o acesso, senhas, e outras informações de cunho pessoal além de deixar vulnerável seus acessos a e-mail, e outros via internet. (ITISHASHI 2011).

No entanto, esse tipo de programa é usado em grandes empresas para monitorar acessos dos funcionários. Porém em mãos erradas se torna uma arma muito perigosa. Um outro mecanismo, semelhante ao descrito acima, é o Wireshark, no entanto esse programa monitora redes sem fio, oi seja o wi-fi (MORAES 2010).

Um método muito utilizado também é o Hoax, esse tipo de haker ou vírus é um mecanismo que divulga falsas histórias ou conteúdos alarmantes, muito visto nos dias atuais. Esse tipo de vírus é o que mais se vê, pois ele chama a atenção por mecânicos muito excitante, tais como opinião política, assinatura de baixo assinado, sim ou não para algum projeto de Lei, logo pessoas com raciocínio lógico a menos ou leigo até acabam caindo e respondendo, colocando dados pessoais e outros. O qual passa de forma direta para os criminosos dados sigilosos e abrindo de certa forma seu computador para os demais vírus.

Convencido da veracidade da página o usuário fica propenso a fornecer seus dados ou executar certos códigos maliciosos, que podem instalar um spyware em sua máquina e fornecer ao cibercriminoso dados que podem prejudicar a vítima.

Em se tratando de e-mail e divulgação, esse mais específico nessa área se chama Phishing, inicia-se com com uma mensagem fraudulenta pedindo dados e acesso da internet como senhas acesso bancário entre outros. Logo também aparece mensagens tais como motivacionais pedindo para baixar o arquivo para ser mostrado ou até mesmo autoajuda ou ajuda para outras pessoas com deficiências pedindo acesso doações entre outros (LAU 2006).

Aos afetados por esse tipo de ação maliciosa GAGLIANO distaca que:

> Em outras palavras, a voluntariedade, que é a pedra de toque da noção de conduta humana ou ação voluntária, primeiro elemento da responsabilidade civil, não traduz necessariamente a intenção de causar o dano, mas sim, e tão somente, a consciência daquilo que se está fazendo. E tal ocorre não apenas quando estamos diante de uma situação de responsabilidade subjetiva (calcada na noção de culpa), mas também

> de responsabilidade objetiva (calcada na ideia de risco), porque em ambas as hipóteses o agente causador do dano deve agir voluntariamente, ou seja, de acordo com a sua livre capacidade de autodeterminação. Nessa consciência, entende-se o conhecimento dos atos materiais que se está praticando, não se exigindo, necessariamente, a consciência subjetiva da ilicitude do ato (GAGLIANO; PAMPLONA FILHO, 2010, p. 70).

Logo vejamos que o conhecimento mais que minímo sobre o tema proposto ou sobre códigos malicosos, fazem com que evitem certos problems judiciais e penais mais a frente, pois acabam entrando no mesmo caminho das pessoas que fazem esse tipo de prática ilícita e quem divulga, mesmo não sabendo a fundo o ato infracionário, acaba sendo responsábilizado de forma indireta pela públicação do mesmo.

1.3 COMO FUNCIONA A INVESTIGAÇÃO DO CRIME CIGERNÉTICO

O presente tópico tem como motivo exlpicar como funciona a investigação contra as pessoas que praticam qualquer tipo de ato ilícito através da internet, desta maneira vale-se ressaltar que tudo se inicia com a criação da Lei que permita a penalização do presente ato, após isso, caberá a polícia monitorar e investigar em conjunto com o Ministério Público e do judiciario por final realizar toda a tramitação para o caso seja devidamente punido (TAVARO 2016).

Em mesmo entendimento TAVARO explica de forma objetiva que:

> O inquérito policial vem a ser o procedimento administrativo, preliminar, presidido pelo delegado de polícia, no intuito de identificar o autor do ilícito e os elementos que atestem a sua materialidade (existência), contribuindo para a formação da opinião delitiva do titular da ação penal, ou seja, fornecendo elementos para convencer o titular da ação penal se o processo deve ou não ser deflagrado. Pontue-se que a Lei no 12.830/2013, ao dispor sobre a investigação criminal conduzida pelo delegado de polícia, deixa consignado que a apuração investigativa preliminar tem como objetivo apuração de circunstâncias, materialidade e autoria das infrações penais (art. 2o, §1o) (TAVORA, ALENCAR, 2016, p. 127).

Em seguida deve-se questionar sobre a competência para julgar os presentes casos, desta maneira é inevitavel apresentar o entendimento do STJ que:

> Trata-se de entendimento firmado pela Terceira Seção do Superior Tribunal de Justiça (STJ), no CC (Conflito de Competência) 97201. Para o Tribunal da Cidadania, no caso dos crimes virtuais, praticados pela internet (neste caso específico calúnia praticada em blog jornalístico) a competência é firmada pelo lugar de onde partiu o ato delituoso. Em outras palavras, local da sede do provedor do site.(BRASIL STJ 2020).

O impacto de se conhecer a competencia se destaca para a investigação também, pois trata-se de crime que pode ser práticado em qualquer lugar até mesmo fora do pais, haja vista a internet nos tempos atuais não possuir mais limitações em relação a fronteiras.

Em mesmo entendiemtno o Código de Processo Penal estabelece em seu artigo 70 que:

> Art. 70 A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução.
>
> 1º Se, iniciada a execução no território nacional, a infração se consumar fora dele, a competência será determinada pelo lugar em que tiver sido praticado, no Brasil, o último ato de execução.
>
> 2º Quando o último ato de execução for praticado fora do território nacional, será competente o juiz do lugar em que o crime, embora parcialmente, tenha produzido ou devia produzir seu resultado.
>
> 3º Quando incerto o limite territorial entre duas ou mais jurisdições, ou quando incerta a jurisdição por ter sido a infração consumada ou tentada nas divisas de duas ou mais jurisdições, a competência firmar-se-á pela prevenção. (BRASIL CPP 1941).

Como pode-se notar, a competência se dá para julgamento no local onde foi práticado o crime, sendo aplicado ao infrator o cunho do julgado daquela região, porém se destaca que mesmo praticado aqui no Brasil o crime e a pessoa ter se refugiado fora do pais, o julgado sera nacional.

Em seguida o artigo 80 do mesmo dispositivo CPP estabelece que:

> Art. 88. No processo por crimes praticados fora do território brasileiro, será competente o juízo da Capital do Estado onde houver por último residido o acusado. Se este nunca tiver residido no Brasil, será competente o juízo da Capital da República. (BRASIL CPP 1941).

Nota-se que apesar da doutrina considerar o inquérito apenas procedimento simplles administrativo, se torna imprescindivel a sua utilização para nortear o julgamento do presente caso, evitando assim decisões arbitrarias desnecessarias.

Na visão investigativa do inquérito, temos que ficar atento a sua relevância para o desenrolar do processo, pois em alguns casos, existem julgados que dispensam o inquérito, tornando o processo fragil a interposições de teses contrária a prisão.

Desta maneira o CPP estabelece em seu artigo 12 e 39 que:

> Art. 12. O inquérito policial acompanhará a denúncia ou queixa, sempre que servir de base a uma ou outra
>
> Art. 39. O órgão do Ministério Público dispensará o inquérito, se com a representação forem oferecidos elementos que o habilitem a promover a ação penal, e, neste caso, oferecerá a denúncia no prazo de quinze dia (BRASIL CPP 1941).

Desta maneira, fica claro que poderá ser dispensado o inquérito porém, a Constituição torna-se contraria a este entendiemnto, ficando baseado nos termos do artigo 144 que:

> art. 144, § 1º, I: apurar infrações penais contra a ordem política e social ou em detrimento de bens, serviços e interesses da União ou de suas entidades autárquicas e empresas públicas, assim como outras infrações cuja prática tenha repercussão interestadual ou internacional e exija repressão uniforme, segundo se dispuser em lei;
>
> art. 144, § 4º Às polícias civis, dirigidas por delegados de polícia de carreira, incumbem, ressalvada a competência da União, as funções de polícia judiciária e a apuração de infrações penais, exceto as militares. (BRASIL Constituição Federal 1988).

Como pode-se ver, o trabalho investigativo tem como primasia o desenrolar dos fatos, para que seja realizado u, julgamento justo e devidamente embasado em provas e outros meios probatórios (COBRA 1969).

Em entendpao com o supracitado, ALBUQUERQUE explana que:

> Ao que parece, sem ação efetiva e competente da Polícia Civil, que é a que investiga e que incomoda o criminoso, tornando sua vida um tormento e coletando provas para fundamentar as condenações judiciais, não se faz segurança pública. No Ceará, de fato, a Polícia Civil, até pelo contingente inexpressivo, e pelo mau gerenciamento e péssimas condições de trabalho, representa carta de alforria para os

> assaltantes, Desenho : Gráfico CNMP Desenho 1: Fonte: Conselho Nacional do Ministério Público nosso maior temor. Com efeito, livrado o flagrante, o que quase sempre ocorre, basta ao ladrão, após meia hora, mudar de bairro ou de esquina e ficar livre para cometer novos crimes impunemente. Não se deseja negar a importância da PM – invenção brasileira, diga-se – mas sim combater o erro antigo e inaceitável da falta de priorização da reestruturação da Polícia Civil, como unidade responsável pelas investigações e, portanto, pela coleta das provas que permitirão o julgamento, pelas vias legais. Em todos os países o combate à violência urbana se deu com a atuação da Polícia Cívil (ALBUQUERQUE Pg 44 2014).

Outro ponto relevante a investigação policial para casos de crimes na internet, é o fato da população não corroborar com denuncias entre outros, pois o medo predominante de falar com a polícia ainda é visto desde os tempos antigos até os atuais. Desta maneira o cunho investigativo se torna limitado, as Leis que impedem alguns tipos de investigação mais afundo dependem de aprovação entre outros meios de liberação para chegar ao destino final que é o criminoso (COBRA 1969).

O conjunto investigatório como ja dito depende de alguns fatores até mesmo do Poder Judiciário, assim GOMES estabelece que:

> Diferentemente do que pode acontecer em outros ramos do Direito, nos quais o Estado se satisfaz com os fatos trazidos nos autos pelas partes, no processo penal (que regula o andamento processual do Direito penal, orientado pelo *princípio da intervenção mínima*, cuidando dos bens jurídicos mais importantes), o Estado não pode se satisfazer com a realidade formal dos fatos, mas deve buscar que o *ius puniendi* seja concretizado com a maior eficácia possível". (Gomes pg 80 2018).

Assim sendo, as investigações necessita de investimento em mecanismos que possibilitam ir a fundo nos sistemas operacionais dos hakers e de pessoas com intenções malicosas, desta maneira o Poder Executivo deve smepre estar se atualizando com equipamentos e equipe adequada para auxiliar na investigação desse tipo de crime (CAVALCANTI, 2009).

A precariedade nesse tipo de investigação se torna muito visivel, conforme DANIEL (2017), explica que:

> Nota-se que a velha política de segurança pública de tentar combater o crime com medidas clássicas, tais como o aumento do número de policiais militares, não funciona mais. O crime há muito tempo se organizou e, se o Estado não investir com inteligência na inteligência da polícia investigativa para que os criminosos sejam identificados e

> levados à justiça, de nada vai adiantar aumentar o efetivo da Polícia Militar nas ruas. Isso por uma razão muito simples: é impossível que tenhamos policiais em todos os lugares e também os criminosos não querem conflitos diretos com o aparato de segurança do Estado. Os criminosos atuam onde a polícia não está, pois sabem que, de fato, não serão investigados, ou seja, se não forem presos em flagrante, não serão depois. Isso gera para a população um sentimento de impunidade e desestímulo até em noticiar os crimes que sofre, pois do que vai adiantar perder horas em uma delegacia a espera da realização de um B.O. se aquele crime não será investigado? Gera ainda um efeito contrário para o criminoso, o qual passa a se sentir estimulado a cometer novos crimes (DANIEL Pg 70 2017).

Voltando ao tópico, a investigação se inicia apartir da denuncia sobre a matéria criminosa, logo após o Ministério Público promovendo o acordo de prosseguimento com o caso, instaura-se assim o processo e inicia-se todo o percurso procesual de respnsabilidade delituosa. Nota-se que no mesmo entendimento de Daniel (2017), os crimes c ibernéticos serão sempre repercutidos até a polícia se instaurar base dentro desse tipo de sistema, pois o crime só acontece onde a polícia não está.

Em entendimento contrario BARBALHO (2021) explica que:

> o problema não está na dispensabilidade ou não do inquérito policial. De fato, o inquérito serve como filtro pra impedir processos infundados. Mas também há casos de flagrante, em que a justa causa está evidente e não há necessidade real de se estender em uma busca probatória que não seja a judicial. O real problema probatório no Brasil está na falta de rigidez dos magistrados no momento de analisar a justa causa para receber a denúncia, bem como na importância que é dada aos elementos colhidos na esfera policial e na iniciativa residual probatória do juiz. Se resolvidos esses problemas, a dispensabilidade seria apenas uma ferramenta para maior celeridade, sem prejuízos às garantias fundamentais (BARBALHO Pg 6 2021)

Dessa maneira identifica-se que a repercussão sobre quais problemas são relevantes para a investigação ou para o processo, percebe-se que a doutrina ainda se encontra em divergencia, merecendo destaque a qual prevalece que é a necessidade do inquérito para o desenrolar do processo.

Por fim, veja-se que necessáriamente o procedimento investigativo merece ser estudado mais a fundo em questão de investimento polícial, aqui, referece ao poder de polícia intesgatória, a procura de mecanismos que visam identificar e rastrar criminosos cibernéticos.

2. ANALISE JURÍDICA SOBRE O CRIME CIBERNÉTICO

A tecnologia sofreu um avanço significativo com o advento da internet. A expansão é notória quando observamos que os meios de comunicação ficaram mais evoluídos e acessíveis a um percentual maior da população. Comprar, conversar com os amigos e até mesmo namoros vem acontecendo pela rede. Hoje em dia é absolutamente normal e possível.

A internet veio pra ficar, mas diante de toda essa facilidade, os crimes nesse cenário tomaram forma mais sutil e estão se tornando bastante corriqueiro, crescendo a cada dia, fazendo mais vítimas e transformando o ambiente virtual um local perigoso e repleto de armadilhas. Para os crimes desta categoria, em virtude de ser um lado novo também no mundo jurídico, não existe uma nomenclatura correta.

Desta forma esses delitos são denominados também de Crimes Virtuais, Crimes Digitais, Crimes Computacionais dentre vários outros tipos. Para que haja um melhor entendimento, se faz necessário compreendermos o conceito de crime sob a égide do Código Penal Brasileiro. De acordo com Lima Carvalho (2014 apud CAPEZ, 2008):

> [...] material, como "todo fato humano que, propositada ou descuidadamente, lesa ou expõe a perigo bens jurídicos considerados fundamentais para a existência da coletividade da paz social". E, formal, onde o "crime resulta da mera subsunção da conduta ao tipo legal e, portanto, considera-se infração penal tudo aquilo que o legislador descrever como tal, pouco importando o seu conteúdo"

Já no conceito analítico, o crime informático, que também é uma espécie de delito cibernético é "toda ação típica, antijurídica e culpável, cometida contra ou pela utilização do processamento automático de dados ou transmissão". (VELLOSO, 2015 apud Ferreira, 2000, p. 210).

E já partindo dos conceitos acima citados sobre crime, Da Silva (2014, p 34), relata que:

> Importante destacar, que os crimes cometidos em meio ambiente virtual ou contra os dados e sistemas de funcionamento de uma máquina informatizada, são consequência da evolução dos equipamentos de comunicação eletrônicos/informatizados e da internet

Conforme já fora dito anteriormente, grande parte dos doutrinadores não possui um consenso no que tange este instituto, entretanto existe também uma classificação bem evidenciada nas literaturas atuais. Seguindo o que diz Velloso (2015 apud Corrêa, 2000b, p. 43), os crimes cibernéticos, são "todos aqueles relacionados às informações arquivadas ou em trânsito por computadores, sendo esses dados, acessados ilicitamente, usados para ameaçar ou fraudar". É importante destacar que, de acordo com o que foi colocado no parágrafo anterior, o ato delituoso seria contra a máquina, o computador em si, ou seja, crimes cometidos contra os dados existentes no dispositivo

2.1 CRIMES CIBERNÉTICOS PUROS

Os Crimes Cibernéticos puros são aqueles em que o agente necessita imprescindivelmente do computador para realizar ataques remota ou diretamente com uso de sistemas informáticos todo o bem jurídico já tutelado. Nesta situação estão envolvidas não só a invasão e captura dos dados salvos em massa, mas também a intenção de alterar, inserir, adulterar ou destruir dados existentes no computador. Nesta linha de pensamento, Carneiro (2012 apud Viana, 2003, p. 13-26), diz que "São aqueles em que o bem jurídico protegido pela norma penal é a inviolabilidade das informações automatizadas (dados)." Ainda nesse contexto, Carneiro (2012 apud Damásio, 2003) se posicionam da seguinte forma

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

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

Fazendo uma análise sobre a acepção desta palavra, podemos concluir que esta é a pessoa que detém um conhecimento singular acerca do assunto e que não necessariamente o use com o propósito de atuar na ilegalidade porque a partir desse discernimento conclui-se que o domínio no referido assunto pode ser visto de forma positiva e negativa.

Já os crackers são pessoas que agem focando a vantagem ilícita. Eles invadem e destroem sites, sejam eles quais forem, fazem quebra de senhas, desenvolvem softwares capazes destruir várias máquinas ao mesmo tempo.

2.2 CRIMES CIBERNÉTICOS IMPUROS

Os crimes cibernéticos impuros ou impróprios são aqueles que são praticados com o uso do computador. Diferente dos crimes cibernéticos puros, esta forma de delito usa o computador como um mero instrumento para a realização deste. Entretanto, os crimes que são realizados com este “auxílio” já são tipificados pelo Código Penal Brasileiro demonstrando que o uso do PC não é um fator primordial mais sim uma das diversas formas de materializar uma conduta delituosa que já está tutelada. Desta forma, Carneiro (2012, apud Damásio, 2003) demonstra:

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

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

3. PERÍCIA DA COMPUTAÇÃO

A perícia da computação apesar de semelhante a investigação, aqui iremos falar do mecanismo propriamente dito, de como chegar ao equipamento e colher as informações precisas para o desenvolvimento do processo investigativo e processual.

Desta forma, Machado explica que:

> A ciência forense usa uma base metódica para chegar a conclusões adequadas às informações disponíveis. Assim, dados e informações serão analisadas e estudadas objetivando algumas conclusões como a identificação de pessoas, locais e eventos, e a correlação entre esses elementos e o fato investigado. Contudo, na realização de exames envolvendo dispositivos de armazenamento, há diversos desafios a serem superados pela perícia como, por exemplo, a quantidade de arquivos. (MACHADO, PG 20 2011)

Conforme visto até agora, sabe-se que o avanço tecnológico da investigação ainda se encontra atrasado, pois ainda não se tem umna efetividade maior em casos que aparentimente tem grande incidência no dia a dia da população. Assim sendo, destaca-se que a perícia é um mecanismo utilizado para descobrir fatos escondidos ou impossiveis a olho nu.

Em julgado pelo entendimento jurisprudencial da Procuradoria Geral da República dispos evento tratativo sobre a pericia digital conforme visto abaixo:

> MPF promove Seminário de Perícia Digital e Crimes Cibernéticos em Brasília
>
> Procuradoria Geral da República
> O evento será aberto para o público interno e externo, com o objetivo de debater os desafios enfrentados em perícias digitais e nas investigações de crimes cibernéticos nacionais e internacionais....O objetivo do seminário é aumentar o conhecimento sobre as áreas de atuação da perícia digital e de Tecnologia da Informação, além de promover a conscientização sobre os crimes cibernéticos, a partir

> de...Ele abordará os desafios internacionais em casos de crimes cibernéticos e perícia digital.

Logo em seguida, ficou firmado a seguinte indagação

> É possível fazer a análise gráfica E SE AFIRMAR, COM CERTEZA, entre o material colhido do punho da autora e UMA MERA CÓPIA DIGITALIZADA do documento a ser analisado, A "PRESSÃO", BEM COMO O "CALIBRE", OS "MÍNIMOS GRÁFICOS" E OS "MOMENTOS GRÁFICOS", dentre outros elementos importantes que na cópia digitalizada não constará, por se tratar de outro papel onde o instrumento escritor (caneta ou similar) não tocou?

A perícia digital é um ato muito delicado, pois em alguns casos serão analisados somente aquilo que foi pedido pelo juiz, dependendo assim da morosidade judiciária para o desenrolar da investigação, se limitando ao poder investigatório.

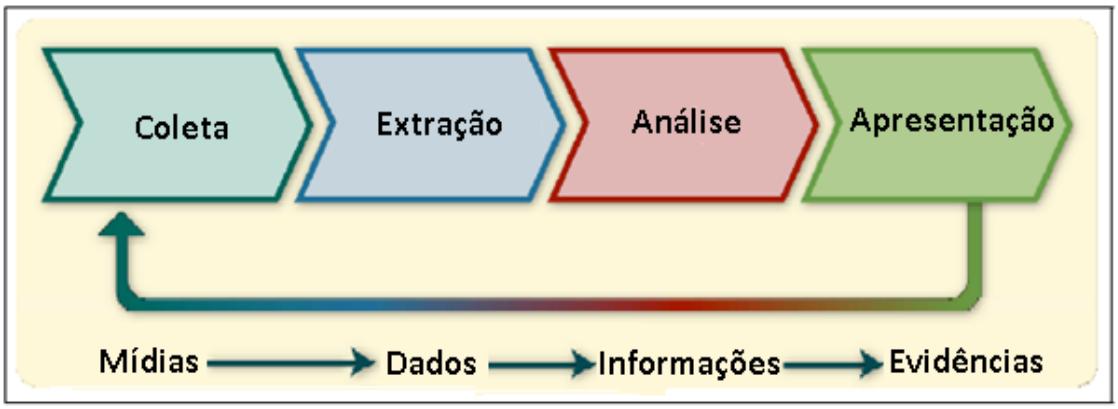
Não somente isso, o doutrinador Gonçalves esclarece que:

> A inovação constante do parágrafo único do art. 927 do Código Civil é significativa e representa sem dúvida, um avanço, entre nós, em matéria de responsabilidade civil. Pois a admissão da responsabilidade sem culpa pelo exercício de atividade que, por sua natureza, representa risco para os direitos de outrem, de forma genérica como constar do texto, possibilitará ao Judiciário uma ampliação dos casos de dano indenizável (GONÇALVES, 2009 pg 70).

Apesar dos avanços em relação a alguns pontos sociais, temos ainda alguns meios contraditórios, tais como visto acima, apesar da investigação depender da justiça, a responsabilização de tal ato recai sobre o poder de Polícia, desta feita ficando algumas lacunas abertas a adversidade de entendimentos sobre o proposto.

A coleta de dados através de investigação digital, é semelhante a uma investigação comum, porém com pontos que devem ser respeitados, pois bem, são fragmentados em etapas, sendo elas ilustradas abaixo:

Tabela 1 - Método de Fundamentação para investigação digital



Fonte: Kent. Et. Tal. 2006.

Vejamos que cada etapa representa um percurso a ser traçado com muito rigor, pois a coleta é a etapa onde se retira da fonte o conteúdo malicioso, aqui neste ponto inicia-se a questão sobre a dependencia do poder judiciário para prosseguir com a investigação e a aprovação das provas colhidas. Após a extração, neste ponto, onde será retirado aquilo de cunho pessoal com aquilo que é ato ilícito, ou seja a separação de dados recolhidos. Ja a analíse é o procedimento jurisprudêncial e entendimento criminosos sobre o ato lesivo e por fim após passado todas as etapas se forma a apresentação de tudo por meio processual demonstrado e juntado ao processo criminal (Kent pg 58 2006).

Desta forma o auxilio com técnicos da computação se torna imprescindivel para o desenrolar dessas etapas, ou seja, no entendimento de Rabelo dispõe que:

> Disciplina autônoma, integrada pelos diferentes ramos do conhecimento técnicocientífico, auxiliar e informativa das atividades policiais e judiciárias de investigação criminal, tendo por objeto de estudo dos vestígios materiais extrínsecos à pessoa física, no que tiver de útil à elucidação e à prova das infração penais, e ainda, a identificação dos autores respectivos (RABELO, 1996, p. 20)

A dependencia dos tecnicos em computação se torna uma chave combinada com o poder de polícia, logo o delegado não precisa saber exatamente tudo sobre computação, pois aqui tratamos que necessáriamente deve-se conter tecnicos e pessoas capacitadas para destrinchar sem ferir nenhum direito do réu em relação a investigação e aos meios de comprovação procesual do ato praticado.

Neste mesmo sentido, vejamos o entendimento de BARROS:

> Nesse sentido, a produção de provas passa ser requisito básico e insubstituível para a própria realização do direito material. E impõe-se que as provas sejam claras, seguras, e aptas a transmitir a necessária confiança ao julgador, de modo que, livre de qualquer dúvida, este possa firmar a convicção racional da existência do fato criminoso e de sua autoria, pois, em sentido inverso, restringindo-se o conjunto probatório aos limites da verdade provável, forçosamente inviabiliza-se a aplicação da pena, restando apenas a solução da ação penal com base no in dubio pro reo (BARROS, 2002, p. 113)

Apesar da utilização de investigadores genéricos para todos os casos, deve-se ser observado que necessáriamente necessita de uma equipe especializada para a investigação do presente caso destacado neste trabalho, pois os crimes cibernéticos são aqueles que acompanham as atualizações diarias.

Outro ponto a ser analisado é o anonimato muita das vezes disponivel por sites que mantem o código de privacidade entre seus acessadores, portanto até onde se torna limitavel esse tipo de investigação e onde será possivel a analise de forma arbitraria.

Em mesmo sentido Silva explana:

> Essa liberdade, aliada a um possível anonimato, passa ao usuário a falsa impressão de que a internet é um território sem lei, um ambiente social paralelo guiado pela total ausência do Estado e de seu poder de polícia. A vida real e a internet seriam dimensões distintas e, portanto, as regras do mundo real não valeriam no mundo virtual (SILVA, 2012, p.1)

Contudo deve-se sempre pensar que a analise precial virtual ou perícia digital, é um procedimento que busca diminuir os casos de fraudes desenvolvidos por hakers que aproveitam desses mecanismos virtuais para ter acesso a dados importantes e pessoais de cada pessoa.

Assim sendo, é imprescindivel destacar o entendimento conceitual de Vecchia:

> A Perícia Digital utiliza um conjunto de técnicas e procedimentos com embasamento científico para coletar, analisar, e apresentar as evidências encontradas. Tem o objetivo de buscar informações relativas a eventos passados em uma investigação (não apenas criminal ou cível, mas também em casos particulares nos quais não se deseja acionar a polícia ou a justiça, em um primeiro momento. A partir da análise dos eventos ocorridos é possível reconstruir as ações executados nos diversos equipamentos e mídias questionados (VECCHIA, 2014, p. 77).

A coleta de daos deve sempre respeitar algumas limitações de tempo. Pois bem, nota-se que a perícia computacional é bem rigorosa, disso ja sabemos, a doutrina é clara a respeito

de suas limitações do poder de investigar, porém a necessidade de pessoais em conjunto para fazer essa análise é necessáriamente devida, pois o conhecimento informático cumulado com o conhecimento da Lei, forma-se assim a perícia ideal para os casos de crimes cibernéticos.

Em outro momento, Machado explica:

> cuidados especiais devem ser tomados durante a coleta dos vestígios digitais, pois assim como alguns vestígios convencionais, são muito sensíveis, uma vez que podem ser facilmente perdidos e/destruídos. O impacto, a umidade, a imersão em água, o calor excessivo, o atrito e o eletromagnetismo são apenas alguns exemplos de possíveis causas de perdas de informações digitais. Após a coleta, precauções também devem ser tomadas durante o transporte e armazenamento do material apreendido (ELEUTERIO, MACHADO, 2010, p. 26)

Por isso se destaca novamente que os tecnicos para a analise e coleta desses dados, pois sua facil destruição ou perda no caminho é muito corriqueiro, haja vista ter alguns mecanismos de auto-destruição. Como dissemos neste trabalho, os hakers são pessoas que estão sempre buscando se atualizar e em mecanismo de defesa contra investigação isso também acontece, sendo muito delicado cada situação.

Alguns outros parametros são faceis de ser identificados porém dificil de responsabilizar alguèm para o assunto divulgado, em alguns casos é possivel ser identificado por redes sociais, tais como instagran e outros que deixam aberturas para divulgação e propagação de mensagens abertas.

Neste caso Júnior relata:

> Artistas, políticos e outras personalidades públicas são constantemente alvo de ataques á moral, à imagem, vítimas de acusações e alvo de insultos através dos canais da rede. Abundam pela rede sites do tipo “eu odeio Sandy e Júnior”, “eu odeio funk carioca ou eu odeia a Telefônica”, de nítido conteúdo ofensivo, ou com informações falsas ou distorcidas: o site Gatas Gostosas, através de imperceptíveis processos de montagem digital, exibe a foto de artistas famosas em cenas de sexo explícito que as mesmas nunca protagonizaram na frente das câmeras (GOES JÚNIOR, 2001, p.147).

Apesar das mensagens serem nitidamente ofensivas, alguns termos de responsabilidades autorais divulgados pelos aplicativos de redes sociais, deixam claro sua omissão na divulgação, priorizando a livre expressão e demais termos proibitórios de divulgação de dados. Pois bem, aqui fica a lacuna sobre auxilio á investigação.

Neste momento,o autor levanta o seguinte caso hipotético; imagine que em

determinado aplicativo de compra e venda, um usuário se utilize de meios fraudulentos para aplicar golpes de vendas falsas que nunca chegarão ao destino, neste caso o provedor do aplicativo ou do site que foi divulgado, tem informações relevantes sobre o acesso, tais como o IP do usuario onde essa sequência de numeros pode ser rastravel pela polícia, ou seja, indo até a pessoa que esta aplicando este golpe.

Em caso concreto, existe uma comunidade onde foram denominados como ANONIMUS, que tem por cunho objetivo, divulgar informações pessoais de políticos entre outros, alguns apoiadores sobre o presente caso se tornan relevantes, pois aqui, referece-se a uma pratica criminosa porém com cunho informativo, mas não deixando o dolo de lado.

No mesmo sentido, a sensibilidade ou o facil acesso a esses dados se dá por conta do não conhecimento sobre a matéria descrita, conforme entendimento de AYRES:

> fato esse causado pela falta de conhecimento e técnicas das forças de segurança pública, e de cultura da população quanto à importância de tal preservação, algo que muitas vezes coloca em xeque a credibilidade dos procedimentos periciais realizados (AYRES, 2015, p. 40)

Assim sendo, algumas das empresas que deixam esse tipo de dados vazar, deixa claro a fragilidade no sistema de segurança, nesse mesmo sentido o doutrinador STUMVOLL explica que:

> Este princípio , baseado na cadeia de custódia da prova material, visa proteger, seguramente, a fidelidade da prova material, evitando a consideração de provas forjadas, incluídas no conjunto das demais, para provocar a incriminação ou a inocência de alguém. Todo o caminho do vestígio deve ser sempre documentado em cada passo, com documentos que o oficializem, de modo a não pairarem dúvidas sobre tais elementos probatórios. A documentação correspondente a cada vestígio pode ser realizada por anotação ou despacho do próprio perito que o considerou (STUMVOLL, 2014, p.10)

Observa-se que a fragilidade na segurança acaba sendo apenas de cunho material e relacionado ao dano moral apenas, mas para a polícia que vai a fundo nas investigações a responsabilidade administrativa acaba sendo mais pesada que para os legitimos responsaveis pelo crime propriamente dito.

Logo, alguns pontos devem ser revisto sobre esses casos, desta maneira, criou-se a Lei Geral de Proteção de Dados, o qual promulga que:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
>
> Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. (Incluído pela Lei nº 13.853, de 2019) Vigência
>
> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
>
> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (Lei Geral de Proteção de Dados Pessoais (LGPD). (Redação dada pela Lei nº 13.853, de 2019) Vigência)

De acordo com a Lei LGPD, pode-se ver que a ecxistência de mecanismo Legislativo mais abrangente sobre a proteção contra hakers, bem como a responsabilização sobre o vazamento de dados só se deu no ano de 2019, e ainda sim muito discutida pois necessáriamente é um ponto novo ainda no ordenamento jurídico merecendo mais destaque sobre cada caso em particular.

Em memso entendimento, o STJ em cartilha no ano de 2022 destacou que:

> A Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709, de 14 de agosto de 2018) foi aprovada em 2018 e entraria em vigor a partir de 14 de agosto de 2020. Houve pedido de adiamento da vigência da lei para maio de 2021, mas a proposta foi rejeitada pelo Congresso, entrando a legislação em vigor em 18 de setembro. A lei representa um marco histórico na regulamentação sobre o tratamento de dados pessoais no Brasil, tanto em meios físicos quanto em plataformas digitais. Além de mudar a maneira como instituições privadas coletam, armazenam e disponibilizam informações de usuários, a LGPD é destinada às instituições públicas – portanto, deve ser seguida por União, estados, Distrito Federal e municípios.
> Logo após a publicação da LGPD, o Conselho Nacional de Justiça (CNJ) editou a Recomendação 73/2020, que orientou os órgãos do Poder Judiciário a adotarem medidas para a adequação dos tribunais às disposições da legislação de proteção de dados.
> Desde então, o Superior Tribunal de Justiça (STJ) tem realizado estudos, promovido discussões e implementado ações voltadas para o

> cumprimento da LGPD e a garantia de proteção dos direitos fundamentais de liberdade e de privacidade dos cidadãos (STJ 2022 cartilha ref. LGPD.)

O ponto buscado nesta cartilha é que os dados relacionados a processos tais como vinculação de dados pessoais, são privativos, ou seja, alguns pontos são abertos, pois existe a incidência do Poder Público sobre as informações, porém a limitação da privacidade de dados pessoais tais como RG, CPF e alguns outros serão devidamente guardados e não divulgados.

Em mesmo entendimento doutrinário, Nogueira exemplifica a quinta geração do Direito o qual seja:

> Quinta geração: são os direitos provenientes da internet e da tecnologia. O direito ao acesso e à difusão da informação são os pontos centrais e a liberdade de expressão volta a ser tratada nessa geração (NOGUEIRA, 2012, pg.207).

Pois bem, neste sentido, procura-se entender que o direito em suas evoluções chegou-se na modernidade, portanto, sempre deve acompanhar a evolução, nessa geração temos que notar que é uma geração que sempre será cobrada no universo que vivemos hoje, pois a informação virtual por meio de redes de internet predomina nos tempos atuais e deve permanecer por longas gerações.

Mesmo sentindo tras o doutrinador Lotufo:

> Nessas circunstancias, para fins de responsabilidade, é muito importante se ter que mais das vezes tem-se admitido nas nossas cortes que as violações cometidas devem ser reparadas, não estabelecendo-se censura prévia, mas estabelecendo forma de indenização, que pode envolver dano moral, cuja composição não é só o denominado preço da aflição, porque cada vez mais o mundo passa a ter uma forma de compreensão, que não se restringe a servir de exclusivo mecanismo de sanção para o infrator, mas também na forma de indenização cabal daquela dor, para que ela não exista mais. Deve, também, ser sancionatória, de tal sorte que seja de uma só vez, como indenização e que também de sanção para que não se repita o dano moral pelo mesmo ofensor (LOTUFO, 2001, p.240)

Por fim, entende-se que a perícia computacional é um mecanismo forte para a elucidação de casos de crimes cibernéticos em todos os seus generos e especificidade, haja vista a coleta de dados e suas analises, descartando aquilo que seja prejudicial ao processo e focando no caso concreto do fato ilícito.

4. CONSIDERAÇÕES FINAIS

Todo o trabalho foi desmistificado, com seus objetivos alcançados e as Leis trazidas foram totalmente analisadas e com conceitos e entendimentos de doutrinadores diferentes e visões diferentes sobre a ótica do tema proposto. desta forma, o crime cibernético é algo muito relevnte e deve ser estudado com mais rigor, o qual passa sempre por atualizações sendo uma das mais atualizadas é a LGPD, Lei de proteção de dados, o qual busca alterar e limitar dados bem como sancionar e trazer segurança para os usuarios de internet.

Por fim, o trabalho se encontra claro a respeito da criminalização dos crimes cibernétivos, no entanto conceitua que esse crime na verdade se trata de uma qualificadora ou atenuante, o que busca trazer mais penas mais severas para quem se aproveitar dos mecanismos de internet para praticar qualquer crime.

REFERÊNCIAS

D´URSO, Patrícia Donati. STJ **analisa competência para os chamados crimes informáticos (crimes virtuais = cybercrimes)**: 2017. competência territorial do local de hospedagem do site Disponível em: <http://www.lfg.com.br/public_html/article.php?story=20110426113540900&mode=print> Acesso em 26/06/2022

CARVALHO, Alexandre. **Phishing faz o Brasil liderar ranking de ataques aos dados bancários**. 2006. Disponível em <http://www.sucesumg.org.br/index.php?option=com_content&view=article&id=230:phishing-faz-o-brasil-liderar-ranking-de-ataques-aos-dados-bancarios&catid=45:ultimas-noticias&Itemid=1> Acesso em 26/06/2022

DAMÁSIO, Eduardo. **Senado aprova projeto de lei para crimes cibernéticos**. 2003. Disponível em: <http://g1.globo.com/Noticias/Tecnologia/0,,MUL641696-6174,00-SENADO+APROVA+PROJETO+DE+LEI+PARA+CRIMES+CIBERNETICOS.html> Acesso em 26/06/2022

MILAGRES; AURÉLIO DE ALMEIDA CAMARGO SANTOS . **As múltiplas faces dos Crimes Eletrônicos e dos Fenômenos Tecnológicos e seus reflexos no universo Jurídico** – SP. 3 ed. 2016

PAESANI, Gustavo Testa. **Aspectos jurídicos da internet**. 3. ed. rev. e atual. São Paulo: Saraiva, 2000.

TOLEDO, Ivette Senise. **Direito & Internet: Aspectos Jurídicos Relevantes**. 2 ed. São Paulo: QuartierLatin. 2017

SILVA. Crimes de Informática: **A Ameaça Virtual na era da Informação Digital, in Internet: o direito na era virtual**/ Luís Eduardo Schoueri, organizador. Rio de Janeiro: Forense, 2016.

SCHECHTER NETO, Mário e CHAVES GUIMARÃES, José Augusto. Crimes Na Internet: elementos para uma reflexão sobre a ética informacional - R. CEJ, Brasília, n. 20, 2016.

VELLOSO Manuel Pedro, **Estudos jurídicos em homenagem a Manuel Pedro Pimentel – SP**: Revista dos Tribunais 2015