PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

ESCOLA DE DIREITO E RELAÇÕES INTERNACIONAIS

NÚCLEO DE PRÁTICA JURÍDICA

COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO

MONOGRAFIA JURÍDICA

VULNERABILIDADE DIGITAL E A PROTEÇÃO DO INDIVÍDUO

ORIENTANDO – BRUNO HENRIQUE BORGES DE OLIVEIRA

ORIENTADOR - PROF. DR. JOSÉ QUERINO TAVARES NETO

GOIÂNIA

2020

BRUNO HENRIQUE BORGES DE OLIVEIRA

VULNERABILIDADE DIGITAL E A PROTEÇÃO DO INDIVÍDUO

Monografia Jurídica apresentado à disciplina Trabalho de Curso I, da Escola de Direito e Relações Internacionais, Curso de Direito, da Pontifícia Universidade Católica de Goiás (PUC - GOIÁS).
Prof. Orientador – Doutor José Querino Tavares Neto

GOIÂNIA

2020

CAPITULO I – VULNERABILIDADE DIGITAL E A PROTEÇÃO DO INDIVÍDUO

Com a evolução da tecnologia o mundo não é mais o mesmo, surge então uma nova espécie de bem jurídico para o direito amparar. O direito e a informática devem caminhar lado a lado, tendo em vista a necessidade que a cada dia se torna mais essencial, principalmente neste tempo de pandemia, onde a tecnologia está sendo peça fundamental para quase todos os meios de produção continuarem girando a economia.

1.1. DIREITO E O MUNDO DIGITAL

O mundo desde os primórdios funciona como uma engrenagem, e a principal parte para a evolução social é a harmonia entre os povos. E quando se fala em harmonia entre os povos, podemos lembrar do Direito, pois é o instrumento da lei que ajuda o relacionamento entre a população, e que de fato é essencial para a evolução social.

Nota-se uma instabilidade social acompanhada de fanatismo nos tempos atuais, fato este que gera desequilibro político, social e econômico. Vivemos em um século onde a tecnologia vem trazendo diversas mudanças, entretanto, há de se ressaltar a importância da dosagem para mergulhar no mundo digital, pois há várias camadas digitais que ao decorrer do acesso desenfreado se torna perigoso para o usuário.

A evolução do direito deve estar em consonância com o progresso que se encontra na sociedade moderna, devido as facilidades e aberturas que o meio digital nos proporciona, pois hoje pode-se pagar uma conta bancária por meio de aplicativos sem sair de casa, ou até mesmo verificar multas de trânsito.

É válido citar o seguinte trecho:

> Essas facilidades estão tão em evidência no cotidiano que não há uma percepção clara de que se vive em uma sociedade informatizada, onde os dados fluem a velocidades inimagináveis há alguns anos, e tudo isso influi em nos valores sociais e econômicos (LISBOA, 2016, p. 10).

As barreiras digitais são praticamente nulas, pois hoje é plenamente possível realizar uma reunião com pessoas de cada país, e isto é um grande avanço

no ramo da comunicação, visto que as gerações dos anos 50 ou 60 sequer sonhavam em poder falar com algum familiar em outro continente.

É válido e importante citar no presente trabalho sobre a visão de Jean Paul Jacob, cientista da IBM, onde é perfeitamente colocado o ponto de vista sobre essa evolução extraordinária, disse o seguinte:

> Sabemos que por mais que a indústria automobilística evolua, jamais irá de São Paulo ao Rio de Janeiro em menos de duas horas; por mais que a medicina evolua, jamais se poderá ressuscitar os mortos... Quanto à informática, nenhuma previsão pode ser feita. (GOUVÊA, Sandra. 1997, p. 39).

Ainda que o direito tenha um mecanismo de resolução de lide mais atrasado quanto as relações que são desenvolvidos no meio digital, é importante que tenhamos sempre pesquisas direcionadas a expansão de uma justiça que seja realmente eficaz principalmente no meio digital onde é comum as pessoas pensarem que é uma ‘’terra’’ sem lei. Portanto, fica claro e absolutamente cristalino a urgência de maiores pesquisas no meio digital para diminuição dos crimes digitais.

1.2 CRIMES DIGITAIS E SUA FREQUÊNCIA

A tecnologia, sem dúvidas, trouxe um nível de vida jamais visto. Um dos avanços mais relevantes vivenciados pela humanidade foi o surgimento da internet. Karen Moraes diz o seguinte: ‘’podemos dizer que vivemos em uma era digital que influencia os setores da sociedade, comércio, política, serviços, entretenimento, informação e relacionamentos ‘’ (KOHN, MORAES, 2007, pg. 05).

Entretanto, não há que se dizer sobre garantia 100% eficaz quanto a segurança do indivíduo que embarca no mundo digital, pois é fato que com o uso frenético da tecnologia houve também consequências trazendo sérios riscos para as pessoas. A facilidade de ocultar a sua identidade através da Internet, atrai diversos tipos de criminosos, tanto tradicionais como ocasionais. Lindolfo Pires Neto:

> A facilidade de transmissão de dados proporcionada pela rede está trazendo muita inquietação aos legisladores de todo o mundo, uma vez que os criminosos que utilizam da Internet estão, na maioria das vezes, acobertados pelo anonimato, dificultando a sua identificação pessoal, assim como sua localização. (NETO, 2009, p. 11).

Visto que o meio digital é uma terra onde existe a facilidade de se ocultar, se torna um meio bastante utilizado para o cometimento de crimes. Infelizmente existe

aquele ar de impunidade que acaba sendo um estímulo impressionante para a evolução do crime na internet.

O âmbito penal com a aceleração da tecnologia foi obrigado a fazer uma área especializada apenas para o meio digital, então surgiu as delegacias especializadas para o combate a esse tipo penal. Todavia, mesmo com o surgimento de algumas delegacias especiais, ainda há uma precariedade para que a população tenha acesso pleno ao aparato investigativo e judicial do Estado. A maioria dos crimes nem sequer são investigados até mesmo pela falta de confiança que a população tem em relação à justiça do país.

É válido ressaltar que conforme a sociedade evoluiu, novos bens acabaram necessitando de proteção jurídica, a exemplo da liberdade cibernética, do comércio eletrônico, vida privada, intimidade, e direitos autorais na internet. O Direito, portanto, têm que acompanhar a evolução da sociedade, e já que tem migrado para o espaço digital, para lá o direito também deve se voltar. O Direito penal informático deve procurar proteger como bem jurídico as informações:

> Está claro que a denominação mais precisa para os delitos ora em estudo é "crimes informáticos" ou "delitos informáticos", por basear-se no bem jurídico penalmente tutelado, que é a inviolabilidade das informações automatizadas (dados) (VIANNA, 2001, p.33).

É importante que a segurança de dados sejam requisitos imprescindíveis a serem observados por todos os órgãos, e nesse momento vê-se a importância da regularização e da criação de tipos penais cibernéticos.

1.3 – O QUE É O CRIME DIGITAL

A caracterização desse tipo de espécie criminal não é simples, em detrimento do desenvolvimento acelerado que as tecnologias atualmente apresentam. Estamos tratando de uma doutrina que está sendo moldada, ainda não é pacífico a jurisprudência acerca do que poderia ser denominado crime cibernético.

Há diversos nomes para definição dos crimes cibernéticos, de tal forma que não existe uma nomenclatura concreta. Entretanto, o que deve ser observado é o uso de dispositivos informáticos e a rede de transmissão de dados com o intuito de delinquir, lesando um bem jurídico. É importante ressaltar que a conduta deverá conter os 3 elementos que compõem o crime, que seria o Fato Típico, Antijurídico e culpável.

O grande X da questão sobre o espaço da internet é que há diversos delitos cometidos que não estão tipificados, o que torna errado sua denominação como crimes cibernéticos, do ponto de vista da CF e do CP.

‘’Algo essencial para o conceito desse tipo de crime é que os crimes de informática são condutas descritas em tipos penais realizadas por computadores ou contra computadores, sistemas de informação, ou dados nele armazenados’’ (CASTRO, 2003, p. 01).

Surgiu uma evolução da definição de cibernéticos para algo mais expansivo. Uma melhor caracterização para o crime de informática é a que o define como uma conduta que atenta ao estado natural dos dados e recursos oferecido pelos sistemas de processamento de dados, e pela compilação, armazenamento, e transmissão dos dados. O crime de informática, pode ser definido como aquele procedimento que ataca os dados armazenados, compilados, transmissíveis, ou em transmissão. ‘’tal crime requer o manuseio de software e hardware para perpetrá-lo. Portanto, toda conduta típica, antijurídica, e culpável dirigida contra ou pela utilização de processamento eletrônico ou transmissão de dados caracteriza o crime, basicamente’’. (SCHMIDT, 2014, online)

É de se notar que o crime de informática tem como elemento principal na sua forma a presença do dispositivo computacional para a prática das mais variadas condutas ilícitas. ‘’Considera-se cibercrime toda atividade onde um computador é utilizado como ferramenta, base de ataque, ou meio de crime’’ (CASSANTI, 2014, p. 20).

Uma caracterização bem interessante sobre cibercrime que considera a visão das vítimas é a seguinte:

> Ofensas cometidas contra indivíduos ou grupos de indivíduos com a motivação criminosa de intencionalmente prejudicar a reputação da vítima ou lhe causar sofrimento físico ou mental, direta ou indiretamente, usando redes modernas de telecomunicações como a internet (Salas de Chat, Grupos de notícias) e celulares (HALDER, JAISHANKAR, 2011, online).

A Organização para Cooperação Econômica e Desenvolvimento da Organização das Nações Unidas (OCDE) definiu como crime informático qualquer conduta ilegal e antiética não autorizada, que envolva processamento automatizado de dados e/ou a transmissão de dados (REIS, 1997, p. 25). Nota-se a preocupação no contexto internacional das organizações com a caracterização, o conhecimento, e

o combate a esse tipo de crime que pode causar consequências econômicas catastróficas.

Uma definição já passada, embora válida, temos o conceito do Departamento de Justiça dos Estados Unidos, que define esses crimes como qualquer violação das leis criminais que envolvem a necessidade de conhecimentos computacionais para sua realização, investigação e processo (DEPARTMENT OF JUSTICE, 1989, p. 02). Observa-se neste conceito que há a necessidade de conhecimentos especializados.

Nota-se que todas essas definições podem ser aplicadas, embora alguns deles frisem alguma artimanha do delito. Para esse estudo adequado é a definição que considera esses crimes como condutas típicas, ilícitas, e culpáveis, que se utilizam de dispositivos computacionais para ataques a sistemas de informação, com o objetivo de obtenção de alguma vantagem ou acesso indevido.

1.4 – Como se dá a divisão dos crimes cibernéticos

É importante expressar como se dá a divisão dos tipos de crimes informáticos. Existe um tipo que separa os crimes informáticos pelo uso de algum instrumento de informática, onde é dividido pela agressão ao meio digital e também pelo o que contém na mensagem enviada através da rede. José de Oliveira discorre: ‘’Em todas essas modalidades, o bem ou meio informático deve aparecer como elemento típico ou determinante’’ (ASCENSAO, 2002, p.256). Huebner et al ofereceu uma forma de divisão, que por sinal é bastante usada pela literatura do mundo jurídico digital.

Existe uma divisão que classificou os tipos de crimes informáticos em tipos que são caracterizados pelo seu uso de dispositivos informáticos. Abrange os crimes caracterizado pela agressão ao meio informático, e pelo conteúdo da mensagem disponível em rede. José de Oliveira Ascensão fala o seguinte: ‘’Em todas essas modalidades, o bem ou meio informático deve aparecer como elemento típico ou determinante’’ (ASCENSAO, 2002, p.256). Importante citar também o autor Huebner Et Al (2003, p.03) que disponibilizou uma classificação muito importante, pelo fato de ser utilizada pela doutrina, onde o autor separou os crimes cibernéticos da seguinte forma:

> • **Crimes centrados no computador**: São os tipos de crime que apresentam como objetivo primordial o ataque a sistemas computacionais, redes,

> dispositivos de armazenamento, e outros dispositivos computacionais. Como exemplo desse tipo de ataque podemos citar o ataque de negação de serviço e o ataque defacement , que visa alterar uma página web.
> - **Crimes auxiliados por computador**: Nesse tipo de crime o computador é utilizado como uma ferramenta para auxiliar na prática de um crime onde o uso do computador não é estritamente necessário. Esse tipo de crime pode ser considerado como uma forma alternativa de cometimento de infrações tradicionais. Pode-se mencionar como exemplo o crime de estelionato praticado com o auxílio de páginas falsas que simulam um site de instituição bancária, que faz com que alguns usuários se enganem e acessem o site falso fornecendo suas credenciais de acesso ao criminoso, o que pode utilizar tal acesso para obter alguma vantagem indevida, o que geraria um provável prejuízo econômico à vítima.
> - **Crimes incidentais por computador:** Uma atividade criminosa onde a utilização do computador seja incidental ou eventual para a atividade em si. Como exemplo podemos citar a contabilidade do tráfico de drogas ou de qualquer outro crime, no qual o computador é apenas uma nova ferramenta utilizada em substituição a outras ferramentas tradicionais. (*grifo nosso)*

É interessante citar que na doutrina existe uma forma de divisão que expõe sobre crimes de informática impróprios ou próprios. Quando se fala na questão dos crimes que são próprios, podem ser aqueles que tem como objetivo alcançar o sistema computacional, e o exemplo clássico seria quando o hacker invade um site e deixa o mesmo indisponível.

Podemos citar o autor Clayton Bezerra versa da seguinte forma: ‘‘os crimes impróprios são aqueles que utilizam a internet ou os meios tecnológicos apenas como uma ferramenta para realização do ilícito, a exemplo dos crimes de falsificação, de documentos, furto e estelionato’’ (BEZERRA, 2016, p. 17). No âmbito dos crimes impróprios, o objetivo do criminoso é alcançar um bem jurídico diferente.

Destaca-se que as ações prejudiciais poderão ser atípicas ou ensejar em um crime cibernético. Versando sobre o tema, quando se fala sobre a ação prejudicial ser atípica, ela pode até causar prejuízo ou transtorno para vítima através da rede mundial de computadores, entretanto não são tipificados, o que torna mais difícil a sua condenação. Os crimes cibernéticos podem ser divididos em crimes cibernéticos abertos e crimes exclusivamente cibernéticos.

Quando se fala em crimes exclusivamente cibernéticos, estamos falando daqueles que precisam do meio computacional para cometer tal crime (como por exemplo no caso do crime de invasão de dispositivo informático, artigos 154-A e 154-B do Código Penal Brasileiro).

Há uma posição que divide os delitos digitais em quatro tipos, na qual o fundamental bem jurídico a ser tutelado pela lei penal é a inviolabilidade da

informação. Portanto, nos crimes cibernéticos próprios o computador é utilizado como meio para executar o delito, mas não há que se falar na violação da informação, e que seria por exemplo os crimes de ameaça e incitação ao crime.

Quando se fala em crimes mistos, o objetivo além de querer proteger os dados, a legislação também vai abordar o bem jurídico de uma natureza diferente, como por exemplo nos crimes eleitorais, e que é importante ressaltar que no Brasil durante a corrida eleitoral para presidente, houve diversos ataques entre os partidos utilizados fake News por meio digital, que por sinal é uma das estratégias mais utilizadas.

1.5 – SISTEMAS MALICIOSOS MAIS UTILIZADOS

Há diversas ameaças quando se fala em meio digital. São cada vez mais inovadoras a forma como os criminosos agem para ultrapassar a camada de segurança, e isto utilizando diversos tipos de criptografia e códigos nunca pensados.

Tal comportamento delituoso cria a necessidade de estar um passo a frente nas atualizações de mecanismos de segurança. Um mínimo de conhecimento de dessas ameaças é essencial para uma melhor definição e enquadramento no devido tipo penal.

Flávio Tamega diz o seguinte:

> Os vírus são programas ou partes de programas de um computador que se propagam inserindo cópias suas em arquivos ou outros programas. Eles são desenvolvidos para alterar nocivamente e clandestinamente softwares instalados em um computador (TAMEGA, 2003, p. 40).

Quando se fala no vírus que causa ‘boot’, esse mesmo vírus tem como foco esse setor de inicialização ou de boot. Pode-se citar como exemplo quando um usuário insere seu pendrive contaminado no computador, que ao ser infectado pelo vírus de boot, pode ser um foco transmissor de vírus para outros pendrives inseridos posteriormente, espalhando com isso o vírus em diversas máquinas.

Há de se falar também no chamado ‘Botnet’, que é um código malicioso o qual permite a um intruso manipular a distância o computador da sua vítima como se fosse um robô. Ele explora vulnerabilidade dos sistemas operacionais e seus softwares. Normalmente a vítima não sabe que o seu computador está infectado com esse código malicioso e nem que está realizando ataques contra outros computadores.

O botnet estaria relacionado diretamente aos ataques de negação de serviço distribuído, no qual os computadores vão enviar uma requisição para um servidor, e desse modo causa uma sobrecarga tornando seus serviços indisponíveis.

Importante falar também sobre o chamado ‘’Defacement’’, que seria um tipo de ataque realizado com o objetivo de modificar páginas de sites. Normalmente conhecidos como “pichadores” normalmente os defaces realizam seus ataques com o intuito de propagar ideias e convicções políticas, ambientais, religiosas etc.

Com o intuito de realizar as modificações nas páginas ou blogs os defaces costumam explorar erros do servidor Web e vulnerabilidades da linguagem de programação de modo a obter o acesso indevido para alterar o conteúdo do site remotamente.

Vale destacar o famoso vírus que algum tempo atrás era bastante popular, principalmente em Lan House, o chamado ‘’cavalo de troia (trojan horse)’’. A característica desse tipo de código malicioso, permite que o computador do atacante acesse à distância o computador da vítima, permitindo desse modo acesso a dados confidenciais. Com o uso desse programa, é possível ocultar sob a camuflagem de outro programa útil e inofensivo, basicamente, abre a porta dos fundos para acesso remoto ao sistema do indivíduo e dando total controle do computador.

Quando se fala do programa chamado ‘’Keylogger’’, a característica dele é ser um tipo que permite monitorar tudo o que o usuário digita com o teclado do seu computador. Recentemente com atualizações, esses programas permitem não apenas captar as teclas digitadas, mas inclusive tirar fotos das telas do computador, mecanismo utilizado na captura de dados bancários em sistemas que usam teclado virtual,

Já no caso do ‘’Hijacker’’, seria uma forma de código malicioso que rouba o seu navegador web e lhe encaminha a páginas não desejadas. Pode ser utilizado, inclusive, na exibição de propagandas, ou exibições de conteúdo pornográfico ou relacionados a sites fraudulentos.

Há o que causam dor de cabeça também, denominados ‘’Rootkits’’, que são programas que ficam ocultos no computador dos alvos, e que podem ser instalados pelo invasor com acesso físico ao computador, ou remotamente através de outra máquina. A maior dor de cabeça é devido a agressividade da camuflagem, e que muitas vezes ficam por vários meses sem ser detectado.

Para manter essa “invisibilidade”, o rootkit, ao ser lido ou acessado usa um mecanismo de filtragem dos dados para que o sistema operacional ou antivírus não detecte o código malicioso. Comumente, esse software é enviado por e-mail para usuários, que inocentemente copiam o arquivo e o executam na sua máquina. Através de técnicas de engenharia social, o atacante convence a vítima, muitas vezes se passando por uma instituição de credibilidade, a realizarem essas atividades que podem comprometer a segurança do sistema.

Quando se fala em ‘’Sniffers’’, dizemos que são programas que monitoram o tráfego de rede, interceptando e analisando todos os dados que ali trafegam, podendo devido a isso distribuir informações sensíveis do usuário. Os Sniffers podem fornecer informações de login e senha, páginas acessadas, vulnerabilidades da rede, além de outras informações confidenciais como e-mails.

Em grandes empresas ou também de menor porte, pode-se utilizar nos computadores profissionais de uso dos colaboradores o ‘’sniffer’’, entretanto, essa ferramenta em posse de criminosos pode ser a chave forte para os mais diversos ataques.

Vale ressaltar também sobre o ‘’Backdoor’’, que seria um tipo de programa que deixa uma “porta dos fundos”, ou seja uma brecha ou vulnerabilidade que permite que o invasor acesse as máquinas infectadas por esse programa. Há de se ressaltar também um programa bastante famoso na atualidade, talvez tenha outro nome, entretanto, nos anos anteriores era denominado de ‘’Hoax’’, e que seria um conjunto de fake News com contéudo alarmante e falso.

Inventam mensagens como projetos de lei, desastres naturais, conspirações, lendas, pessoas doentes e mensagens religiosas que causam prejuízos para as vítimas. Através dos hoaxs pessoas de boa fé espalham essas falsas informações através de e-mail, sites ou redes sociais. É comum esses boatos virem acompanhados de solicitação para que o receptor encaminhe a mensagem para sua lista de contatos de e-mail através de promessas de prêmios ou de colaboração para uma boa causa como auxílio financeiro a alguma pessoa doente.

A estratégia do criminoso que utiliza o phishing scam é levar a vítima a clicar em um link, que direciona a uma página bastante semelhante a que o usuário espera, como por exemplo a página de um banco.

CAPITULO II – EFICÁCIA DAS APURAÇÕES CRIMINAIS NO MEIO DIGITAL

É fato que vivemos em um país onde os recursos são muitos, porém, não são bem aplicados. Um exemplo seria o investimento na busca de resolução de crimes cibernéticos, onde o Estado se direciona mais a polícia ostensiva (polícia militar), do que na polícia investigativa (polícia civil). Neste capítulo será discutido sobre esse tipo de estratégia política de investimento ostensivo e repressivo.

2.1 – INVESTIGAÇÕES NO CAMPO DIGITAL

É inegável que a frase: ‘’Os dados são o novo petróleo’’ resume os últimos anos da humanidade no meio digital, onde o banco de dados que cada indivíduo detém é uma mina de ouro, tendo em vista a intenção por trás de cada indivíduo.

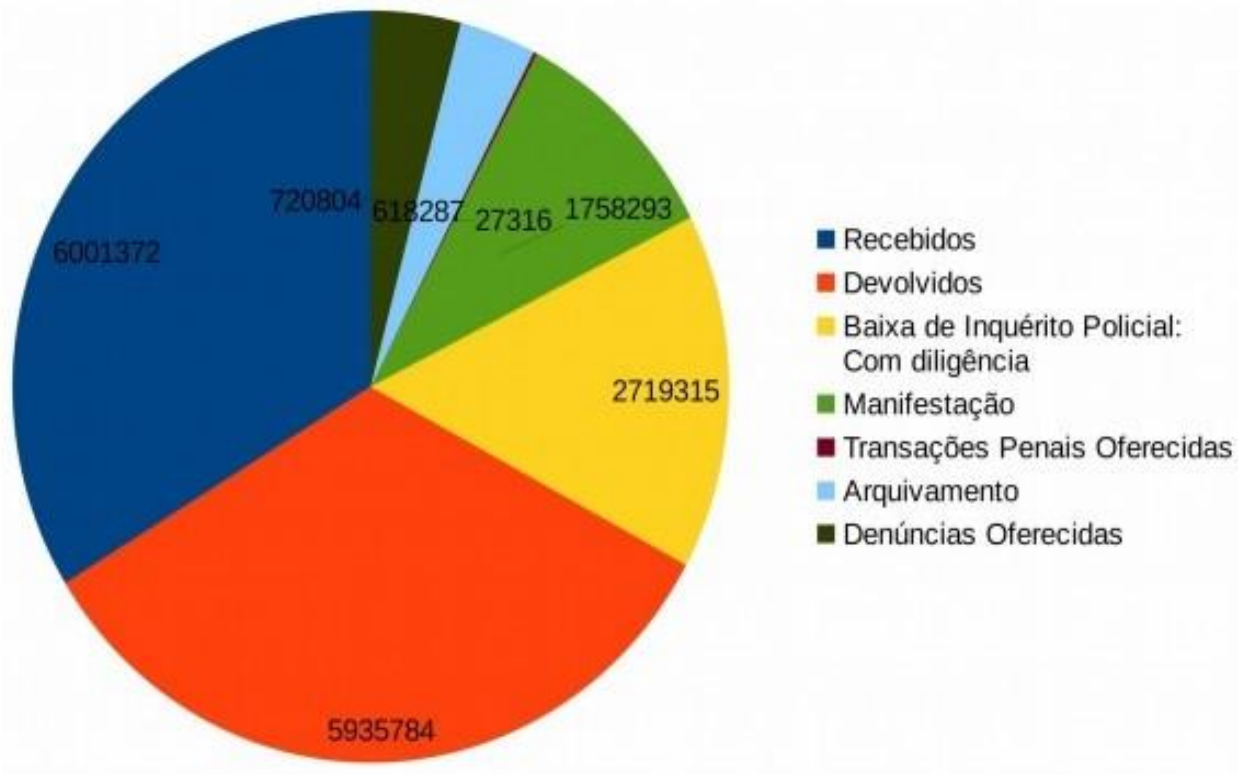
Tendo em vista a produção da legislação penal para averiguação dos crimes no meio digital, existe uma primordialidade para a efetiva função da lei, e consequentemente vem o trabalho do Ministério Público, da polícia e do judiciário.

A investigação criminal faz parte do processo onde é peça chave para a solução de denúncias ou queixas-crime. Segundo doutrina amplamente difundida: ‘’o inquérito policial é o procedimento administrativo presidido pelo delegado de polícia, inquisitorial, informativo, dispensável e preparatório’’ (CAPEZ, 2016, p.148).

A Constituição Federal trata de atribuir as funções investigativas para a Polícia Civil dos Estados, e à Polícia Federal. Tais atribuições são essenciais para o cumprimento efetivo da investigação, visto que a ostensiva é da competência da Polícia Militar. Partindo dessas informações, deve-se fazer o seguinte questionamento: Essas polícias são estruturadas para demanda de crescimento criminal cada vez mais evolutivo? Se comparado a estrutura da polícia atual, com o aparato que o criminoso pode usar, é realmente de igual para igual?

É de ressaltar que a polícia federal apresenta maiores recursos financeiros comparado com a polícia civil, e além disso é uma referência em questões de crimes virtuais. Vale mencionar que a polícia civil tem uma desvantagem quanto aos recursos, pelo fato de ‘’disputar’’ com a polícia militar. O que dificulta o seu trabalho principal, tendo por base a preferência dos governos em um modelo de polícia que além de oferecer uma maior visibilidade, pode ser controlado com mais facilidade.

É quase óbvio que não há a chance de melhores números na redução dos crimes sem o devido investimento nas polícias investigativas. Como é demonstrado no gráfico abaixo o número de inquéritos que são verdadeiramente colocados como processos penais representam uma porcentagem pequena. Isso se explica na grande parte dos casos pela falta de estrutura da polícia judiciária para investigação dos crimes, o que acaba fazendo que grande parte dos inquéritos sejam arquivados pela inexistência de autoria.



Fonte: Conselho Nacional do Ministério Público

Pode-se ressaltar a fala do ilustre professor Cândido de Albuquerque (2014), que versa sobre essa falta de investimento na polícia civil:

> 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, 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 Civil (Judiciária).

É infelizmente um fato que as leis, mecanismos de tecnologia por parte da polícia não são suficientes para acompanhar a evolução da tecnologia, sobretudo porque ela evolui muito rápido. Pode-se afirmar também que as ferramentas da lei não são acessíveis a toda população brasileira, mas mesmo assim precisamos iniciar uma cultura de proteção de dados para evoluirmos e aprimorarmos os mecanismos para encontrar efetivamente o criminoso responsável pelo vazamento de dados ou até mesmo pelo simples acesso a algum documento sigiloso independente do indivíduo.

Há uma exigência muito grande para a averiguação de crimes devido ao fato do sentimento de impunidade, da ausência do Estado. Não obstante deve-se sempre caminhar aquele pensamento que por mais que seja penoso as investigações dos crimes digitais, a administração pública não pode se dar ao luxo de não esgotar todas as formas para a resolução desse tipo de crime.

2.2 – LEI 12.965/2014 E SUA CONTRIBUIÇÃO

O Marco Civil da internet, ou a lei supracitada, tem o objetivo de estabelecer princípios, garantias, direitos e deveres para o uso da internet no brasil e vai determinar consequentemente as diretrizes para atuação da União, Estados, Municípios e o Distrito Federal em relação a matérias, como está disposto no artigo 1º da referida Lei.

É importante citar o artigo 2º e o 3º da referida lei, que versa:

> Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o **respeito à liberdade de expressão**, bem como:
> I - O reconhecimento da escala mundial da rede;
> II - Os **direitos humanos**, o desenvolvimento da personalidade e o **exercício da cidadania em meios digitais**;
> III - a pluralidade e a diversidade;
> IV - a abertura E a colaboração;
> V - A livre iniciativa, a livre concorrência e a **defesa do consumidor**; e
> VI - A finalidade social da rede.
>
> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes **princípios**:
> I - Garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> II - **Proteção da privacidade**;
> III - proteção dos dados pessoais, na forma da lei;
> IV - preservação E garantia da **neutralidade de rede**;
> V - Preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;

> VI - **Responsabilização dos agentes de acordo com suas atividades, nos termos da lei;**
> VII - preservação da natureza participativa da rede;
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.
> Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte. (*grifo nosso*) (BRASIL, LEI Nº12.964, 2014)

É importante citar o artigo 2º e 3º visto que se trata dos fundamentos e princípios que vão ser a base de todo o corpo de normas, a referida lei tem o intuito de manter o equilíbrio no que se refere a liberdade de expressão e tirando a ideia de ‘’terra sem lei’’ que muitos ainda pensam ser assim.

Quando se trata do marco civil da internet, não podemos deixar de lado que há 3 pilares que vão nortear toda sua responsabilidade, que são: a proteção à privacidade do usuário da internet, a garantia da liberdade de expressão e a garantia da neutralidade da rede. É válido ressaltar que o marco civil da internet não tem viés penal, apenas trata no aspecto do direito cível e social.

Para o presente trabalho é importante passar pelo aspecto cível, pelo fato da lei em comento ser considerada a constituição da internet. Pode-se entender quando se fala dos três pilares da referida lei, que a neutralidade da rede é um princípio que garante a não discriminação de toda diversidade de conteúdo que trafega na internet seja pacote de vídeo, som, de fotos.

Se ela não for garantida os provedores de internet podem privilegiar o tráfego de informação e dar preferência para os dados que melhor beneficiarem seu modelo de negócio. Por exemplo, se meu vizinho assinar um provedor e que por não ter que respeitar a neutralidade tem um acordo com o google, o youtube dele irá carregar muito mais rápido que o meu, já que não tenho esse acordo, mas pode ter outros, para outros serviços.

O valor que pagamos hoje para ter acesso a toda diversidade da internet pode valer apenas para um acesso restrito, porque sem a garantia da neutralidade da rede, os provedores poderiam segmentar toda a internet e vendendo esse acesso em vários modelos de planos de assinatura. Por exemplo, um pacote somente para redes sociais, ou outro bem mais caro para ver filmes e etc.

A navegação por toda rede mundial de internet passaria a funcionar como uma tv a cabo cuja diversidade de acesso depende diretamente do bolso do consumidor.

É válido ressaltar, a importância desta lei na internet, tendo em vista a abordagem que a mesma traz quando se fala em princípios e principalmente, sobre a rede mundial de computadores. Basicamente, todas as leis que abordarem o direito digital, terá como base a lei do marco civil da internet.

É importante citar também o contexto histórico que promoveu a criação desta lei. Foi em 2014, no governo de Dilma Roussef, onde o governo americano foi acusado de fornecer dados, tanto de empresas, como de governos e entre eles o Brasil. E como resposta, a então presidenta sancionou a Lei 12.965. E desde então, a referida lei vem sendo usada como base por todo o direito digital.

2.3 – INVESTIGAÇÃO TÉCNICO-CIENTÍFICA DIGITAL

No decorrer da leitura do presente trabalho, é de fácil compreensão que nossa justiça é bastante atrasada. Se o atraso ocorre até para investimento em saúde pública, quiçá o investimento em segurança tecnológica acessível para a população. Afinal, o uso da internet se tornou algo que faz obrigatoriamente parte da vida da maioria da população brasileira e tendo em vista o número gigantesco de pessoas conectadas, se tornou um ambiente que apresenta facilidades para o cometimento de crime, tomando como base o uso simples de uma compra da internet, transações bancárias, redes sociais e entre outras.

Partindo deste raciocínio, pode-se chegar à conclusão que é extremamente necessário que haja segurança para os usuários como a lei do marco civil da internet dispõe. Então, o Estado fica encarregado da investigação criminal andar em sintonia com a perícia criminal, o que está corretíssimo tendo em vista que para incriminar um indivíduo é necessário que se obtenha provas, e se tratando de um meio totalmente virtual, a missão de desvendar o indivíduo por trás da sua tela é algo enigmático principalmente para levar ao convencimento da justiça.

É certo que não há lógica em dirigir um Inquérito Policial não tendo o domínio sobre os princípios que rege a criminalística. E, não obstante, fica difícil o esclarecimento de um crime sem o conhecimento mínimo do Delegado diante a matéria tratada na investigação, que no caso é o direito digital. Não se trata de dominar a área digital 100%, entretanto, deve-se ter uma base para por exemplo, pedir exames específicos de prova obtida e quais requisitos são essenciais.

Cumpre salientar que, mesmo o código de processo penal propagando o princípio chamado de livre convicção do juiz, é evidente a necessidade de produção de provas e quanto mais provas concretas, melhor para haver a ausência de motivos na contestação. É importante citar um trecho de Marcos Antônio 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).

Cumpre salientar a necessidade de uma especialização da perícia em crimes digitais, tendo em vista a peculiaridade de cada invasor e criminoso atrás da tela de um computador. Todo e qualquer vestígio, informação e dados que obtiverem deve ser preservada assegurando a cadeia de custódia para que não se tenha dúvidas sobre as provas. Tal procedimento obedece rigorosamente ao princípio que baseia a criminalística, o da documentação. Vejamos:

> 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).

Quando se trata de busca e apreensão de materiais, seja físico ou digital, o Ministério da Justiça discorre da seguinte maneira:

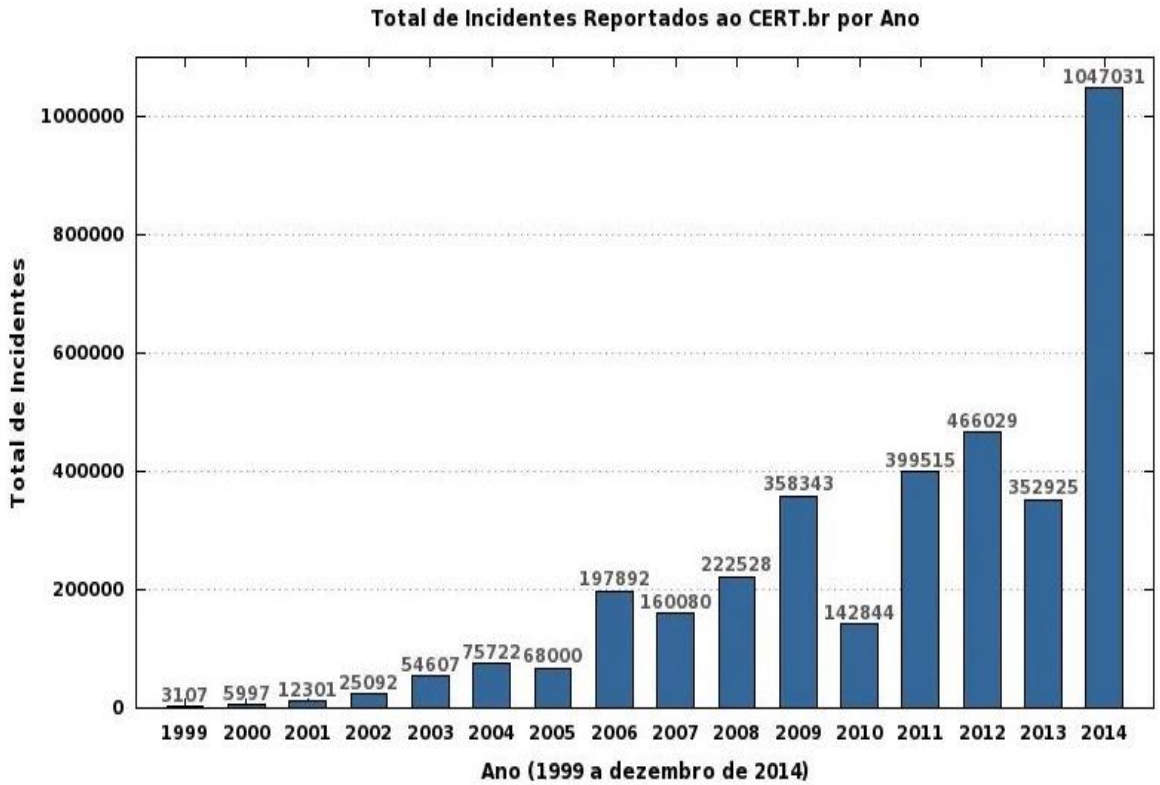
> O trabalho de busca e apreensão requer certas ações a depender do caso concreto. Esse tipo de utilização específica requer na maioria das vezes a utilização de softwares apropriados para essa tarefa. Existe inclusive um procedimento operacional recomendado para a Secretária Nacional de Segurança pública com o intuito de padronizar os exames periciais de equipamentos computacionais (BRASIL, MINISTÉRIO DA JUSTIÇA, 2013, p. 87)

A atuação do perito deve se basear em algumas perguntas. Como por exemplo: O que apreender, a descrição do material apreendido, como transportar o material apreendido, como apreender. Essas peculiaridades na hora da apreensão

são de fundamental importância, visto que são materiais de fácil manipulação do criminoso, e que pode ser alterado a distância dependendo do que a polícia tem como objetivo de investigação.

É importante demonstrar também com números precisos e aproximados, sobre a proporção que os crimes digitais estão tomando desde o começo da tecnologia. Com a demonstração de números fica claro como será difícil para o Brasil se adaptar ao jogo de cintura dos criminosos, até porque atualmente é bastante acessível os conteúdos que incentivam e ensinam como praticar crimes virtualmente, começando pela famosa deep webb.

Vejamos alguns dados sobre o crescimento absurdo de delitos apenas no Brasil:



Verifica-se a razão pelo qual, principalmente os brasileiros, temem usar a internet, tendo em vista que pensam ser uma terra sem lei e infelizmente não confiam totalmente no trabalho do Estado, porém, é compreensível este tipo de opinião quando nos deparamos com dados assustadores de impunidade digital. É certo que é deve do Estado proteger o cidadão, visto que no direito penal há o direito objetivo e o

subjetivo, que especificamente fala a respeito da responsabilidade do Estado e o poder-dever punitivo ante os delitos praticados, seja no âmbito digital ou em qualquer outro.

Como fora demonstrado os dados referente ao número absurdo de crimes, vejamos quais são os mais comuns na categoria de produtos e serviços:

Este tipo de gráfico nos mostra como é bárbaro o número de crimes que ocorrem todos os dias no meio digital, e que infelizmente, a tendência é só aumentar, devido ao fato da teclado que sempre é falada, a ineficácia da lei no caso concreto e a falta de amparo do Estado frente a solução de conflitos que utilizam o meio digital para praticar delitos.

Interessante mencionar um importante marco para os primeiros passos que o Brasil deu na sexta-feira, dia 18/09/2020. Finalmente a Lei geral de proteção de Dados (LGPD) entrou em vigor, e por enquanto o que se sabe é que a nova legislação vai melhor garantir os direitos de cada indivíduo no meio digital, regulando a circulação e concessão de suas informações a terceiros, com transparência e no interesse coletivo. E no caso do empresário, a LGPD vai exigir mudanças na política interna e

externa, pois o empresário deverá tratar os dados de clientes, fornecedores e funcionários com responsabilidade.

2.4 – LEI CAROLINA DIECKMANN

No ano de 2012 fora sancionada a Lei nº 12.735/12, mais conhecida como Lei Carolina Dieckmann. O nome dado a esta lei se dá pelo fato da atriz brasileira ter sido vítima de um ataque cibernético, onde os hackers tentaram extorquir o valor de R$ 10.000,00 da atriz, para que não fosse divulgado fotos íntimas da atriz, entretanto, a mesma não cedeu as ameaças e acabou sendo exposta pelo grupo de criminosos cibernéticos. Tal atividade, além da interceptação de e-mail, se configurou no crime de extorsão.

Com a criação desta lei, foi introduzido ao Artigo 154 do nosso código penal brasileiro o seguinte:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

A referida norma foi um importante passo para o meio digital, entretanto é ainda muito rasa. No momento que verificamos que não há muita discussão na legislação brasileira sobre a invasão de dispositivo eletrônico.

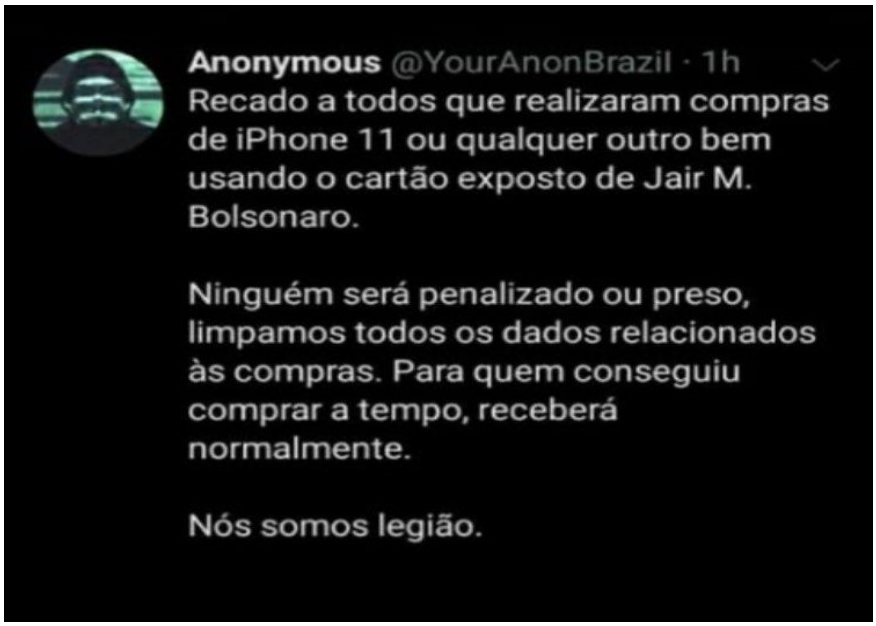
O que se deve colocar em pauta é a complexidade do que o ataque pode gerar para a vítima, tendo em vista que não é raro após o ataque na rede de internet, a vítima suicidar. Há diferentes formas de expor uma pessoa, mas a principal é pelo compartilhamento nas redes sociais e links fantasmas, onde não há maneira eficaz de extinguir todo e qualquer dado que venha ser exposto.

Um exemplo de insegurança digital, foi um momento onde usuários de uma rede social chamada ‘’twitter’’, fizeram uma exposição de dados bancários, dentre elas do presidente do Brasil, Jair Bolsonaro. Onde os internautas começaram a comprar eletrônicos no cartão de crédito corporativo do Presidente. Alguns filmaram os produtos chegando e mostrando os dados do cartão de crédito.

Alguns foram punidos, mas a maioria que não filmaram e mandaram para endereços diferentes do que residem, conseguiram ficar com os produtos e não foram pegos. O que mais intriga nesse tipo de ataque é que decidiram aleatoriamente quem seria a vítima e conseguiram com bastante facilidade.

Este exemplo supracitado foi motivo de vários brasileiros refletirem como estão vulneráveis com ataques cibernéticos, principalmente quando a questão financeira está em jogo. Como já fora dito, não foi algo que demorou meses para ser vazado na internet, e sim algo de poucas horas e o estrago já estava feito. Como a internet é uma rede que conecta pessoas do mundo todo, os dados já haviam sido compartilhados por todo o Brasil.

É válido citar o grupo que vazou e é responsável por uma série de ataques cibernéticos no Brasil e no mundo, o grupo chamado ‘’Anonymous’’. Tal grupo está na internet praticando ataques desde 2003, e seu único propósito é o Cyber ativismo, onde encontram um alvo e expõe dados pessoais, histórias pessoais e diversos dados sigilosos no âmbito penal. Para se ter uma noção do quanto a internet é um mundo complexo, este grupo nunca foi preso pelo simples motivo de não serem rastreáveis, vejamos a imagem de um tweet que o grupo publicou no seu twitter sobre a exposição dos dados bancários do presidente:

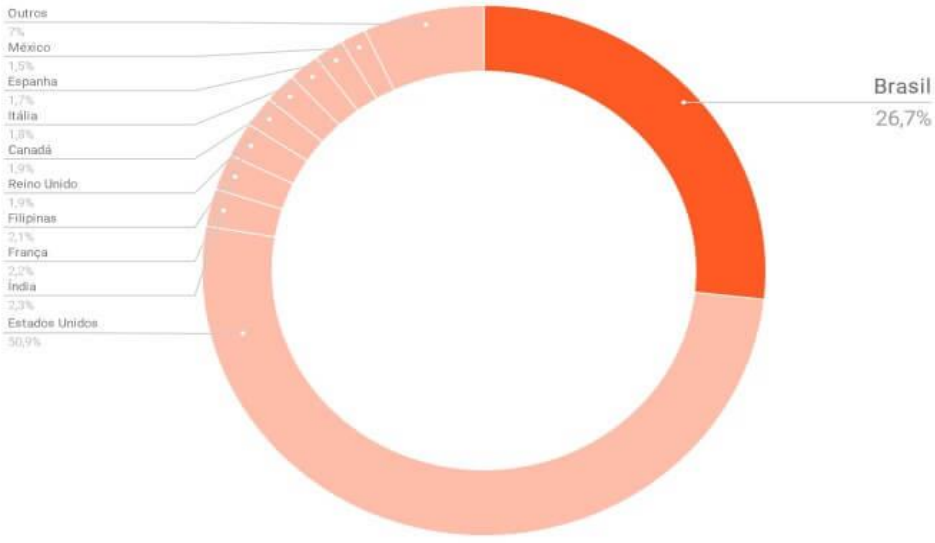


É válido mencionar que não fora apenas o cartão do Presidente, o empresário Luciano Hang, proprietário da Havan, também sofreu o ataque de ter seus

dados bancários exposto. Apenas nesses exemplos citados, devemos ter cautela de como e onde navegamos pela internet, pois como também fora mencionado no capitulo 1 do presente trabalho, existe páginas falsas com a mesma identidade visual de site famosos, com o intuito de enganar o indivíduo e fazer com que a própria pessoa forneça seus dados sem ela sequer saber.

Todo especialista em cibersegurança afirma que nós somos o nosso principal inimigo, tendo em vista que nós mesmo fornecemos todos os dados que o hacker precisa. Um pequeno exemplo seria quando pesquisamos inocentemente algum produto ou serviço na internet e quando vamos para alguma rede social vemos exatamente o produto que procurávamos no google aparecendo em anúncios, e isso é exatamente o que se fala neste trabalho, sobre os termos que aceitamos para usar determinado serviço ou aplicativo, e que muitas vezes somos impedidos de usar caso não permita que o aplicativo acesse nosso dispositivo. Um exemplo de rede social que não permite ser acessada sem ter o acesso ao aparelho eletrônico do indivíduo, é o Facebook.

Como está sendo falado sobre a Lei Carolina Dieckmann, e como esta lei deixa vago o crime de invasão, tendo em vista que é punível apenas a invasão com intenção de vantagem ilícita, não abrangendo no caso de um criminoso que deseja olhar informações da pessoa, mesmo sem o objetivo de uma vantagem direta. É interessante citar aqui também um gráfico que demonstra a quantidade de dados bancários que foram expostas no Brasil no ano de 2019, ficamos atrás somente dos Estados Unidos, vejamos:



No gráfico acima o Brasil teve 26,7% da base de cartões encontrada exposta, ou em números seria o equivalente a 345.674 cartões. É um número preocupante, tendo em vista que a tendência é sempre crescer, pois o criminoso que pratica uma vez e tem sucesso no ataque, irá continuar e pode até ensinar outras pessoas como realizarem o ataque, o que não é nada incomum.